OPTIMIZATION OF MEDICAL IMAGE STEGANOGRAPHY USING N-DECOMPOSITION GENETIC ALGORITHM

BUSHRA ABDULLAH SHTAYT

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2023

Awang Had Salleh
Graduate School
of Arts And Sciences

Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

BUSHRA ABDULLAH SHTAYT AL-SARAYEFI

calon untuk Ijazah **PhD**
(candidate for the degree of)

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

"OPTIMIZATION OF MEDICAL IMAGE STEGANOGRAPHY USING N-DECOMPOSITION GENETIC ALGORITHM"

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada : ***18 Oktober 2022.***
That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: ***18 October 2022.***

Pengerusi Viva: *(Chairman for VIVA)*	**Assoc. Prof. Dr. Massudi Mahmuddin**	Tandatangan *(Signature)*
Pemeriksa Luar: *(External Examiner)*	**Assoc. Prof. Ts. Dr. Nur Izura Udzir**	Tandatangan *(Signature)*
Pemeriksa Dalam: *(Internal Examiner)*	**Assoc. Prof. Dr. Roshidi Din**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Assoc. Prof. Dr. Nur Haryani Zakaria**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Assoc. Prof. Ts. Dr. Nor Hazlyna Harun**	Tandatangan *(Signature)*

Tarikh:
(Date) ***18 October 2022***

Permission to Use

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Sallah Graduate School of Arts and Science. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the Universiti Utara Malaysia for any scholarly use which may be made of any material from this thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Sallah Graduate School of Arts and Science
UUM College of Arts and Science
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Melindungi maklumat sulit pesakit adalah kebimbangan yang kritikal dalam steganografi imej perubatan. Teknik Least Significant Bits (LSB) telah digunakan secara meluas untuk komunikasi selamat. Walau bagaimanapun, ia mudah terdedah kepada ketidakjelasan dan risiko keselamatan disebabkan oleh manipulasi langsung piksel dan pengehadan corak ASCII. Akibatnya, maklumat perubatan yang sensitif terdedah kepada kehilangan atau perubahan. Walaupun terdapat percubaan untuk mengoptimumkan LSB, isu-isu ini terus berlaku disebabkan oleh (1) perumusan pengoptimuman mengalami kekangan tersirat yang tidak sah yang menyebabkan ketidakfleksibelan dalam mencapai pembenaman optimum, (2) kekurangan penumpuan dalam proses carian di mana panjang mesej memberi kesan ketara kepada saiz ruang penyelesaian, dan (3) isu kebolehsesuaian aplikasi di mana data berbeza memerlukan lebih fleksibiliti dalam mengawal proses pembenaman.

Untuk mengatasi kekangan-kekangan ini, kajian ini mencadangkan kaedah yang dikenali sebagai algoritma genetik penguraian-n. Algoritma ini menggunakan carian panjang boleh ubah untuk mengenal pasti lokasi terbaik untuk membenamkan mesej rahsia dengan memasukkan batasan bagi mengelakkan perangkap minimum tempatan. Metodologi kajian terdiri daripada lima fasa utama: (1) penyiasatan awal, (2) merumuskan skema pembenaman, (3) membina skema penguraian, (4) menyepadukan reka bentuk skema ke dalam teknik yang dicadangkan, dan (5) menilai prestasi teknik yang dicadangkan berdasarkan parameter menggunakan set data perubatan daripada kaggle.com. Teknik yang dicadangkan menunjukkan rintangan terhadap analisis statistik yang dinilai menggunakan analisis Statistik Boleh Balik (RS) dan histogram. Ia turut menunjukkan kelebihan kepada ketidakjelasan dan keselamatan yang diukur oleh MSE dan PSNR kepada set data Chest (0.0557, 0.0550) dan Retina (60.6696, 60.728). Namun, jika dibandingkan dengan keputusan yang diperoleh dari teknik yang dicadangkan, penanda aras mengatasi set data Brain oleh kerana sifat imej yang homogen dan latar belakang hitam yang luas.

Penyelidikan ini telah menyumbang kepada penguraian berasaskan genetik dalam steganografi imej perubatan dan menyediakan teknik yang menawarkan keselamatan yang lebih baik tanpa menjejaskan kecekapan dan penumpuan. Walau bagaimanapun, pengesahan lanjut diperlukan untuk menentukan keberkesanannya dalam aplikasi dunia sebenar.

Kata kunci: Teknik steganografi LSB, Algoritma genetik, Panjang berubah-ubah, Ketidakjelasan, Keselamatan.

Abstract

Protecting patients' confidential information is a critical concern in medical image steganography. The Least Significant Bits (LSB) technique has been widely used for secure communication. However, it is susceptible to imperceptibility and security risks due to the direct manipulation of pixels, and ASCII patterns present limitations. Consequently, sensitive medical information is subject to loss or alteration. Despite attempts to optimize LSB, these issues persist due to (1) the formulation of the optimization suffering from non-valid implicit constraints, causing inflexibility in reaching optimal embedding, (2) lacking convergence in the searching process, where the message length significantly affects the size of the solution space, and (3) issues of application customizability where different data require more flexibility in controlling the embedding process.

To overcome these limitations, this study proposes a technique known as an n-decomposition genetic algorithm. This algorithm uses a variable-length search to identify the best location to embed the secret message by incorporating constraints to avoid local minimum traps. The methodology consists of five main phases: (1) initial investigation, (2) formulating an embedding scheme, (3) constructing a decomposition scheme, (4) integrating the schemes' design into the proposed technique, and (5) evaluating the proposed technique's performance based on parameters using medical datasets from kaggle.com. The proposed technique showed resistance to statistical analysis evaluated using Reversible Statistical (RS) analysis and histogram. It also demonstrated its superiority in imperceptibility and security measured by MSE and PSNR to Chest and Retina datasets (0.0557, 0.0550) and (60.6696, 60.7287), respectively. Still, compared to the results obtained by the proposed technique, the benchmark outperforms the Brain dataset due to the homogeneous nature of the images and the extensive black background. This research has contributed to genetic-based decomposition in medical image steganography and provides a technique that offers improved security without compromising efficiency and convergence. However, further validation is required to determine its effectiveness in real-world applications.

Keywords: LSB steganography technique, Genetic algorithm, Variable-length, Imperceptibility, Security.

Acknowledgments

First and foremost, praise and thanks be to Allah, and may prayers and peace be upon His Messenger Muhammad (may Allah bless him and grant him peace). Then, to my dear supervisors, Assistant Professor Dr. Nur Haryani Zakaria, and Assistant Professor Dr. Nor Hazlyna Harun, I am highly grateful for the support and advice you have provided me throughout my research journey. I cannot thank you enough for your guidance and for sharing your wealth of knowledge. Experience has been invaluable and contributed significantly to my personal and professional development. Your advice and insight have helped shape my research and have given me the confidence to pursue new challenges and opportunities.

I interacted with many researchers, academics, and practitioners in preparing this thesis. Therefore, I would like to thank my colleagues without mentioning anyone's name for fear of forgetting one of them, but I believe Allah knows their efforts and puts them in the balance of their good deeds.

I want to thank my family and its members for their support and for enduring hardships throughout the study. To my father's soul, I am asking Allah to have mercy on him. Thanks to my mother's constant prayers, I ask Allah to bless her with health and wellness. Thanks to my brothers, thanks to my sisters, thanks to my nephews (Haider, Abdullah, Karrar). I wish you success and Allah's satisfaction.

I do not know whether the words are enough. My husband, although you are no longer physically with me, your soul and love have remained with me throughout my studies. I cannot thank you enough for the unwavering support and encouragement you have given me, even in your absence. I felt your presence every step of the way; I am grateful for the memories we shared and the strength and resilience you instilled in me. I ask Allah to place you in the position of Mahmoud in the highest heavens.

Last, thanks and appreciation go to all the University of Utara Malaysia staff, especially the College of Computing team, for their support. Thank you all. Allah blesses you all.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ABC	Artificial Bee Colony
ACO	Ant Colony Optimization
AD	Average Different
AI	Artificial Intelligence
AI	Adobe Illustrator
ALSB	Adaptive Least-Significant Bit
ATD	Adaptive Threshold Detector
BMP	BitMap
bpb	bits per byte
bpp	bits per pixel
DCT	Discrete Cosine Transform
DE	Diamond Encoding
DFT	Discrete Fourier Transform
DICOM	Digital Imaging and Communications in Medicine
DISB	Dual Intermediate Significant Bits
DWT	Discrete Wavelet Transform
EALSBMR	Edge Adaptive Least Significant Bit Matched Revisited
Em	Embedding Process
EMD	Exploiting Modification Direction
ePHI/R	electronic patient health information/records
EPRs'	electronic patient records’
EPS	Encapsulated Postscript
Ex	Extraction Process
GA	Genetic Algorithm
GIF	Graphic Interchange Format
GLM	Grey Level Modification
GUI	graphical user interfaces (GUI)
HAS	Human Auditory System
HER	Electronic Health Record

HIS	Hospital Information System
HS	Harmony Search
HVS	Human Visual System
ICT	Information and Communication Technologies
ISB	Intermediate Significant Bit
ISPs	Internet service providers
IWT	Integer Wavelet Transform
JPEG	Joint Photographer Expert Group
LSB	Least Significant Bit
MD	Maximum Difference
MIS	Medical Information System
MSB	Most Significant Bit
MSE	Mean Square Error
NAE	Normalized Absolute Error
NCC	Normalized Cross-Correlation
NP	Non-deterministic Polynomial
OPAP	Optimal Pixel Adjustment Process
PACS	Picture Archiving and Communication System
PCM	Parity Checker Method
PDF	Portable Document Format
PNG	Portable Network Graphics
PSNR	Peak to Signal Noise Ratio
PSO	Particle Swarm Optimization
PVD	Pixel Value Differencing
QoS	Quality of Service
RC4	Rivest Cipher4
RGB	Red-Green-Blue
RMSE	Root Mean Square Error
ROI	Region of Interest
RONI	Region of Non-Interest
RS	Reversible Statistical

SC	Structural Content
SSIM	Structural Similarity Index Metric
TIFF/TIF	Tagged Image File Format
TS	Tabu Search
VLC	Variable-Length Chromosome
VLC-GA	Variable Length Chromosome-Genetic Algorithm
WWW	World Wide Web
X2	Chi-square

CHAPTER ONE
INTRODUCTION

1.1 Introduction

This chapter presents a background of information hiding as a means of information security, primarily technical steganography as a covert communication method. This chapter starts with the research knowledge in section 1.2 and the research motivation in section 1.3. The following section 1.4 includes the definition of the operation. Next, the problem statement, research questions, and objectives are introduced in sections 1.5, 1.6, and 1.7, respectively, followed by the research's scope and the significance behind the research in sections 1.8 and 1.9. This chapter ends with the thesis organization and summary to conclude the chapter presented in sections 1.10 and 1.11, respectively.

1.2 Background of Research

Since the beginning of time, there has been a distinct difference in how humans communicate; they desire communication secrecy. The digital age has ushered in a dramatic shift in how to communicate where interaction and the speedy sharing of information and messages between persons who are sometimes in separate time zones are made more accessible by communication technologies, opening up new options for protecting communication (Onyeator & Okpara, 2019; Kumar et al., 2011). Information security is protecting information from tampering, manipulating, or reducing the probability of risks. For example, money transfers to users' bank accounts and exchanging medical images have become the most security-demanding sectors over the Internet as they require protection services from attackers (Kadhim et al., 2019; Cheddad et al., 2010).

Under the information security umbrella, two main branches are cryptography and information hiding (Abdulwahed, 2020; Subhedar & Mankar, 2014; Chang et al., 2004). Cryptography aims to deny unauthorized access to secret information and satisfactorily scrambles information (Abikoye et al., 2020; Taleby Ahvanooey et al., 2018). Cryptography is the most commonly used, which consists of two main processes: encryption and decryption (Desai & Mali, 2018). Encryption refers to all the processes used to make sensitive data (i.e., plain text) safer and less likely to intercept unauthorized persons by converting ordinary information into an unintelligible form (i.e., ciphertext). At the same time, the reverse is called decryption which generates the original message known as plaintexts (Rakshit et al., 2021). Nevertheless, cryptography's problem is storing the data in encrypted text, which seems unreadable (i.e., hiding the message's meaning). As a result, the attacker can monitor the transfer of information, interrupt it, and use cryptanalysis to infer the message's content and meaning (Kadhim et al., 2019; Mehta & Bhatti, 2019; Qadir & Varol, 2019).

On the other hand, the concealment of information points to a secret communication for transmitting confidential information over a communication channel that conceals the existence of a message (Agarwal et al., 2020; Subhedar & Mankar, 2020; Parah et al., 2012). Information-hiding techniques can achieve a powerful security approach for two reasons. Firstly, it can hide secret information in cover media (e.g., an image, text, video, or audio), resulting in undetectable concealed data (Jansi & Muthusamy, 2020). Secondly, it hides the existence of the secret message, ensuring that only the intended recipient knows the presence of confidential information. This approach to information-hiding technology has recently become important in several areas of real-world application, such

as strengthening the transmission and retrieval of sensitive data of written wills, medical reports, mobile banking reliability, and trade secrets (Kaur et al., 2021; Abdulwahed, 2020).

Information hiding includes two branches which are 1) watermarking and 2) steganography (Nipanikar & Deepthi, 2019; Jung & Yoo, 2015). A watermark is a method for verifying the identity and authenticity of the owner of a digital image by concealing the owner's information within a digital signal or an image (Singh, O. P., Singh, A. K., Srivastava & Kumar, 2021; Thongkor & Amornraksa, 2017; Sarkar & Sanyal, 2014). The watermark inserted into a carrier (i.e., image, audio, or video) is considered related to watermarking. For instance, in a television broadcast Like CW and ABC, NETFLIX, the station logo is visible to the right or left of the screen, and the hospital logo (image watermark) provides authenticity and confidentiality (Kumar & Singh, 2020; Singh & Pradhan, 2019).

At the same time, steganography is a particular state of a general information hiding problem that provides an additional layer of security by concealing sensitive data in other data that may appear insignificant from an attacker's perspective (Din et al., 2018; Laskar & Hemachandran, 2012). The confidential message usually is not related to the carrier object in steganography. Steganography aims to prevent others from knowing the concealed information and remove suspicion by having hidden data and finding a solution to protect communication from being tampered with (Abikoye et al., 2020; Pandey, 2020). Stenographers could utilize digital media to embed confidential data, which has certain redundancy in their representation. "Image Steganography" refers to concealing a secret message within a host image. Image media is regarded as the ablest (Shah & Bichkar,

2019; Atee, 2017; Cheddad et al., 2010) since it is widely published in the media and has a high level of repetition, allowing for data concealment with high possibility.

The difference between cryptography and information hiding is the scramble of the secret message by utilizing a crypto-key to transform the original message (i.e., plaintext) into something with no meaning (i.e., ciphertext). Regardless of the possibility of unbreakable the ciphered, it will excite suspicion, and once the decrypted data is deciphered, the data becomes fully undefended. In contrast, information hiding can enhance existing cryptographic solutions and lighten the mentioned drawbacks by hiding the encrypted data in multimedia content. So, no one can see the confidential information, which can only be accessed by the authorized party (Zeeshan et al., 2017; Katzenbeisser et al., 2015).

1.3 Research Motivation

From an application perspective, steganography is a growing field of interest, especially when most important transactions are now online. Real-world applications include critical domains such as finance, banking, military, medical, and many others (Shibani et al., 2020; Bhagat & Bhardwaj, 2019). Of those critical domains, this research mainly concerns telemedicine application, which involves storing, processing, and transferring a large amount of information, especially in digital images.

The exchange between clinics through open networks is prevalent today, making sensitive data vulnerable to damage and theft, affecting the patient's life and eventually becoming unsafe (Banday & Pandit, 2021; Al-Dmour, 2018). Thus, the exchange mechanism must be robust against manipulation, requiring a secure network (Jansi & Muthusamy, 2020). The purpose is to obtain the patient's medical information, including personal diagnostic

information and images on which the diagnosis is based, rather than separately. Moreover, it saves storage space in the Hospital Information System (HIS) (Wang et al., 2017). The secrecy of the medical reports is essential and sensitive and is at stake. Thus, it is necessary to efficiently conceal the data during transmission via a specific network or even save it on a database (Pandey, 2020; Subhaluxmi Sahoo & Sony Snigdha Sahoo, 2020). The modern healthcare system, such as the Picture Archiving and Communication System (PACS) and the HIS, provides the healthcare section with digital medical information (i.e., medical images) simply and quickly. Technology-enabled E-diagnosis has primarily replaced traditional file-based diagnosis within digital medical imaging systems. Hospital Information Systems (HIS) and medical imaging platforms generate and manage digital images over various modalities, such as Ultrasound, X-ray, Computerized Tomography (CT), Magnetic Resonance Imaging (MRI), etc. (Qasim, 2019). Images captured in a hospital are preserved in the PACS that serve as integrated systems for collecting, archiving, and exchanging medical data.

Medical image is regarded as the core of telemedicine. It is utilized for various purposes, such as diagnosis, training, treatment, remote learning, and medical counseling sessions between clinicians and radiologists (Allaf & Kbir, 2018; Al-shaikh, 2017). However, despite their great utility in modern health care, dealing with digital medical images raises several new security issues via ethical methodology and legal for local archiving and distant medical services (Thabit, 2021). Consequently, even minute changes could affect the doctor's diagnosis; hence, medical images demand a high-security rank to ensure that only genuine change events occur.

Storing, sending, retrieving, or merging data with digital images is difficult because digital data is vulnerable to penetration by unauthorized persons to access this information via Internet transmission to exploit it, either concerning good or immoral aims. Hence, there is an urgent need to present technologies that ensure the safety of medical information will share online. Thus, this research focuses on the steganographic scheme used to protect transmitted medical images.

1.4 Operation Definition

This section intends to provide an operational definition of several terms commonly used throughout this thesis. Definitions and terms have been given of this research in the context as follows::

1. **Security**: It indicates the capability of the steganography system to withstand steganalysis attacks and is considered a successful steganography system; if the attacker fails to detect the hidden (Shah & Bichkar, 2018; Ganesan & Bhavani, 2013).
2. **Imperceptibility** (i.e., quality/undetectability): Human eyes cannot distinguish between the cover and stego images. Stego-image is expected not to have any critical visual artifacts that lead to high-quality stego-image, which implies good imperceptibility (Shah & Bichkar, 2018; Roy & Changder, 2016; Seyyedi & Ivanov, 2014).
3. **Capacity**: It indicates the quantity of data a steganography algorithm can conceal in a particular coverage without generating visual or statistical degradation (Al-Saedi, 2016; Kolli & Vaishakh, 2013; Samima et al., 2013).

4. **Robustness**: It refers to the ability of the secret message to stay intact despite the stego-carrier being subjected to conversion, cropping, filtering, scaling, sharpening, and other attack techniques (Gupta, 2015; Praneetha, 2015; Ghebleh & Kanso, 2014).

5. **Meta-Heuristic Algorithms:** They are nature-inspired optimization techniques according to Darwin's theory of survival of the fittest to find feasible solutions to complex combinatorial optimization problems from various solutions (Kulkarni et al., 2017; Rajesh et al., 2014). The most common meta-heuristic algorithms are Evolutionary Algorithms (EAs) such as Swarm Intelligence (SI), Genetic Algorithm, Harmony Search, and Tabu Search (Agrawal et al., 2021). Glover (1986) coined the term meta-heuristic by combining the Greek prefix meta- which means 'beyond' or 'higher level,' with heuristic from the Greek (euriskein or heuriskein) (Gandomi et al., 2013).

6. **Optimization:** The term "optimization" indicates finding a group of inputs for an objective function whose outcomes maximize or minimize the output (Dhiman & Kaur, 2018; De León-Aldaco et al., 2015; Gendreau & Potvin, 2014). A desire to maximize expected profits or minimize cost, time, and so on of optimization problems in almost all activities of humans. Such as a packing problem, the shortest path problem, and a knapsack problem (Kulkarni et al., 2017; Sorensen et al., 2017).

7. **Local and Global Optimum:** In the search space, a local optimum (optimal) solution is a point where none of the adjacent solutions is better than the current one (i.e., all the neighboring points are worse than the current one). In contrast, a global optimum solution is a point in the search space where every one of the other solution points is worse than or (equal to) the current solution (Gendreau & Potvin, 2014; Talbi, 2009).

8. **Metameric:** It is defined in anatomical biology as a division consisting set of structurally similar parts which are not necessarily identical (Ryerkerk, 2018). Metameric describes a single chromosome's segmented structure of genomes, while metavariable represents each segment (Ryerkerk et al., 2019).

1.5 Problem Statement

Medical image steganography is one of the significant applications of steganography to preserve patient information from manipulation and violation. They are, furthermore, embedding medical information inside their medical image for telemedicine and archiving requirements. Secure transmission of medical information over insecure networks is a vital telemedicine issue. Medical image steganography schemes require more focus on a subset of requirements to prevent tampering with vital patient data, such as imperceptibility and resistance to steganalysis.

Reviewing the literature observed three main steganography domains: spatial, frequency, and hybrid. Among the most well-known spatial steganography techniques is the Least Significant Bit (LSB) technique, which inserts the secret message into selected areas of an image using weight-based selection criteria. This technique helps conceal relatively large amounts of data not visible to the naked eye within the host object. Even at a low embedding rate, it is effortless to detect the presence of hidden messages using steganalysis algorithms. In medical steganography, the quality of the medical image after embedding is crucial for the transmission's intended purpose, which is to preserve diagnostic integrity. Due to significant distortion during the embedding process, medical image quality is incompatible with the large amount of data embedded in the host image,

making the presence of confidential data easily detectable (Karawia, 2021; Mahalakshmi et al., 2017).

For medical images, the spatial techniques, in general, and least significant bits (LSB), in particular, are more appealing due to three factors: (1) the concern about reversibility in the frequency domain, (2) computational complexity in the frequency domain, and (3) the diffusion effect when transforming an image from its frequency domain to its spatial domain, which might cause altering medical information (Khalil, 2017; Al-Dmour & Al-Ani, 2016). However, LSB suffers from two significant weaknesses; firstly, its impact on imperceptibility and capacity due to a direct change in the bits values of the host image. Using more than one bit negatively affects the lack of imperceptibility due to increased distortion of the host image. While the capacity of embedding increases, which is a trade-off to the imperceptibility. Secondly, its detectability is correlated with ASCII letters in the least changed (significant) bits. Hence, improving LSB methods to mitigate LSB's weaknesses (Mahdi et al., 2019; Khan et al., 2016; Chan & Cheng, 2004).

Several mechanisms/approaches have been adopted for optimization; unfortunately, the issues have not been addressed clearly, for many reasons. The first issue is that the formulation of the optimization problem of steganography suffers from non-valid implicit constraints, which might lead to falling into the local minima trap. For example, in work (Kanan & Nazeri, 2014), the message is assumed to be inserted in a connected area, which might not be flexible enough to reach an optimal embedding. The second issue is lacking convergence in the searching process, where the length of the message significantly affects the solution space's size; long messages increase the number of possibilities for embedding. Therefore, reducing the solution space without incorporating non-valid

constraints is needed. The third issue is the nature of steganography applications, where different data types require the user to have more flexibility in the embedding control. This issue is also known as application customizability.

Furthermore, the optimization is regarded as a combinatorial optimization process with the nature of NP-hardness (non-deterministic polynomial-time hardness). Thus, to satisfy steganography's security and imperceptibility requirements, it is necessary to propose a technique to search for the optimal location for embedding secret messages by incorporating some constraints to avoid a local minima trap. Figure 1.1 summarizes the problems to be addressed in the proposed technique of medical image steganography, as shown. The problem has three main issues: (1) the non-valid implicit constraints, (2) the lacking convergence, and (3) the need for application customizability.

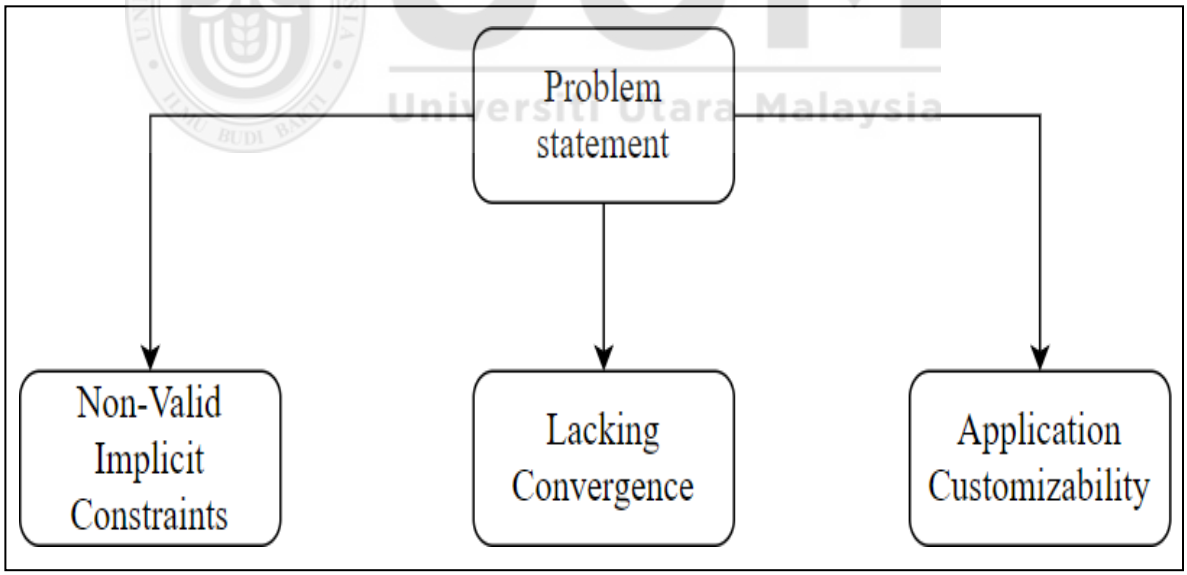


Figure 1.1 The Problem Statement

Therefore, the development of decomposing controlling parameters, message decomposition, and non-contagious embedding is needed to address them. This is

regarded as an optimization approach to improve convergence or cater to the problem of lack of convergence.

1.6 Research Questions

The questions addressed by the research are:

1. How to avoid the issue of non-valid implicit constraints in the optimization of steganography?
2. How to handle the lacking of convergence in the optimization algorithm?
3. What is the controlling parameter for message decomposition, and how to decompose the message?
4. How to integrate the two proposed optimization techniques to address the above issues?
5. How can the proposed optimization technique be evaluated using suitable metrics and scenarios based on selected benchmark studies?

1.7 Research Objectives

This research aims to optimize the LSB for medical image steganography by improving the genetic algorithm. The following are the research objectives to support the aim of this research:

1. To propose a novel formulation of steganography in medical images that avoids non-valid constraints in the optimization for more optimality.
2. To design a decomposition controlling scheme to cater to the lack of convergence and address the application's customizability.

3. To integrate the two proposed schemes into a single by improving GA to address the issues in the LSB technique for medical images.
4. To evaluate the proposed technique using standard evaluation metrics and compare it with suitable benchmark studies.

1.8 Scope of The Research

To achieve security in exchanging medical information over the internet. The medical image has been used in this research as a host for embedding patient information to ensure that critical information is not compromised and manipulated. As a result of the objectives defined above, the scope of the research is determined based on the following:

1. Critical patient information will be embedded, for example, patient identification information and illness type.
2. Image steganography uses corresponding patient information to embed text (patient information) inside an image media.
3. The research utilizes medical images of various types, including Chest, Retina, and Brain, from reputable data sources such as Kaggle and FAU. Data sources are detailed in Chapter 3.
4. This research does not consider rotation, scaling, zooming, and other image manipulation techniques.
5. Multiple criteria, including MSE, PSNR, correlation, histogram, and RS analysis, will be used to assess the performance of the proposed technique. PSNR and MSE were utilized because they provide a metric for comparing the original and stego-image using pixel-wise information.

Figure 1.2. displays the scope of this research, which is used in achieving the desired objectives.

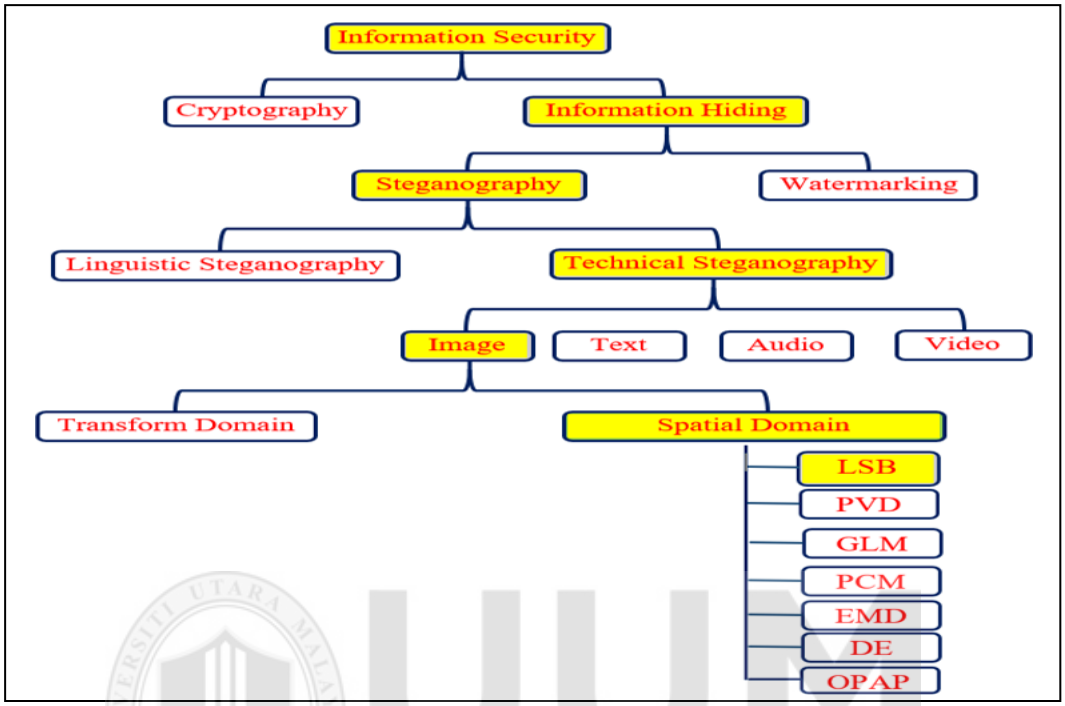


Figure 1. 2 Scope of Research

1.9 Significance of Research

Healthcare establishments have realized the advantages of employing IT-based solutions to manage medical information early. Daily, hospitals help numerous patients, generating vast amounts of data (e.g., patient records, diagnostic information, and medical images). Citizens visit many health establishments and undergo medical tests during their lives, necessitating the need to keep all of this history. In this research, electronic information within the modernistic health information infrastructure benefits medical service providers, including augmenting patient autonomy, enhanced clinical treatment, and advances in public health control and health research.

Quality in healthcare is one of the main concerns, and healthcare is considered a critical point. The hold on the history of patient information was the motivation behind the

emergence of numerous Electronic Health Record (EHR) systems. EHRs have improved healthcare information management by keeping track of patient demographics, past medical history, admission notes, symptoms, and medications. The information-hiding techniques participate in the medical service improvement that is supplied to people through many sides, including:

1. Hiding techniques helped health care systems exchange medical information remotely for various purposes to contribute to the rapid treatment of patients.
2. Provide the significant aspects of medical image steganography in telemedicine, including imperceptibility and security. The medical image's quality, including the patient's information, addresses the security issue.
3. Besides hiding techniques, optimization algorithms search for the best location to embed the patient's confidential information in their medical image. For example, as in this research, a genetic algorithm improves the LSB substitution method to achieve imperceptibility and security for medical images.

The proposed technique may save time and cost by combining the patient's data with their medical image and sending it for remote medical consultation, contributing to the patient's early treatment.

1.10 Thesis Organization

This thesis is organized into six chapters as follows; the first chapter introduces the concept of information security and its main branches, which are (cryptography and information hiding), the critical requirements to address issues for telemedicine, and the motivation behind this research. Then, the research questions, objectives, scope, and

significance are followed. The chapter's conclusion includes the proposal's organization and summarizing the chapter.

Chapter two summarises the information security techniques, including information hiding and cryptography methods for protecting confidential data via an open network. It also discusses the essential features of steganography systems, particularly the methods used, such as spatial and transform domain and their characteristics, and reviews them intending to propose an approach for achieving security. Furthermore, this chapter contains a survey of the relevant literature on the steganographic system. General methods and popular criteria are applied to measure the basic requirements for medical image steganography, such as imperceptibility and security, discussed in this chapter.

Chapter three shows the steps of the methodology used to achieve this research's objectives. Every step of the method briefly describes and discusses the key features of achieving the objective and thus gives a logical sequence to accomplish the next objective.

Chapter four explained the proposed n-DGA image steganography scheme, including many phases: data preparation, including the secret message and host image, embedding process, validation, and extraction process.

Chapter five shows the simulation results and discusses the evaluation of the proposed n-DGA technique to achieve the research objectives in imperceptibility and security.

Chapter six finalizes the thesis with a summary, Findings, contributions, limitations of the work, and future work and recommendations.

1.11 Summary

This chapter starts with addressing the domain area, which then highlights the related issues or problems. A few research questions were derived based on the topics discussed, leading to some research objectives being set forward. The scope of this research is stated to define the boundary of the work that will be carried out later. Also, it highlights the significance of conducting this research, driving the motivation further to improve the existing issues highlighted earlier in this chapter. The next chapter will further the discussion of the literature review to set the forward state of the art for the domain area of this research.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

Protecting patient information is the most significant priority for any electronic health system because tampering with medical data leads to misdiagnosis. The significant developments in digital technologies and communications have increased the exchange of telemedicine services, aiming to transfer and exchange medical information and images between doctors, consultants, and health institutions to consult; however, hackers may be compromised. This chapter introduces an overview of telemedicine applications and information security systems in sections 2.2 and 2.3. Next, section 2.4 introduces steganography systems. Then, section 2.5 presents the steganography methods, and image steganography is presented in section 2.6. The most important evaluation criteria for the performance of the image steganography method have been presented in section 2.7. Furthermore, the datasets in section 2.8 were used to compare the proposed and benchmark techniques. Lastly, sections 2.9 and 2.10 are illustrated the related work and a summary of this chapter, respectively.

2.2 Telemedicine Application Domain

The expansion of information and communication technologies (ICT) and their advanced adoption by healthcare providers have enhanced knowledge of diseases and treatments, contact between professionals, workflow, and process efficiency, enabling high-quality service delivery in general (Sugathan, 2016; Holden & Karsh, 2010). Recent and rapid advancements in communication technologies have made the transfer of significant amounts of electronic data simple and efficient (M. A. Usman & M. R. Usman, 2018; M.

A. Usman et al., 2017). developments have resulted in several advantages, but it is also necessary to consider several risks and dangers.

Telemedicine utilizes ICT to provide clinical health care from afar space. The word telemedicine is derived from the Greek prefix 'tele,' which implies distance, and its full definition is remote medicine (Fatehi & Wootton, 2012). Technologies such as telemedicine are developing daily, and holding the security of medical data has become defying (Usman, M. A et al., 2017). Furthermore, capturing medical data by unauthorized people has become a big cybercrime. If critical data were stolen or captured unauthorizedly, it could infringe on fundamental patient rights. A Hepatitis patient, for instance, does not wish to share information with unauthorized parties. Consequently, confidential and data integrity protection against use and unauthorized access is required.

Ago its early adoption, it has altered how physicians define and manage health information, allowing for more interactive storage and retrieval of vast quantities of clinical data. Nevertheless, sharing electronically protected health information/records (ePHI/R) and radiographs for consultation and diagnostic purposes poses confidentiality, originality, and identified risks. These medical records contain sensitive information about the patient's condition, necessitating absolute security during transport and storage (Rashid et al., 2018; Olanrewaju et al., 2013).

Telemedicine and image protection require methods and techniques to safely share ePHI/R and system radiographic images (Swaraja, 2018; Astuti & Wisety, 2015). The main benefits of telemedicine using steganography are:

(a) These methods do not require additional memory storage because ePHI/R is embedded within the cover (i.e., radial images).

(b) To transmit data, embedded ePHI/R into the cover radiographic images are shared so that no extra bandwidth requires for ePHI/R transfer.

(c) ePHI/R embeds in the X-ray; hence, no one can detect its existence in the X-rays. These methods are secure for keeping data private.

Unfortunately, the rapid development of health informatics has also introduced new challenges. For example, the incredible amount of daily data is now a burden for healthcare establishments, which must expend significant infrastructure budgets to store and manage this data (Mathivanan et al., 2018). Several researchers as Ratib et al., 2016; Sugathan, 2016; Bellon et al., 2011, have worked on infrastructure management and big data cost-cutting solutions for the healthcare industry. Some healthcare foundations have adopted telemedicine solutions to provide remote services for less specialized human resources establishments. Despite its economic and social advantages, telemedicine has yet to minimize record execution and irregular adoption, with sluggish and fragmented acceptance of daily health care operations. Rapid information and communication technology (ICT) developments have recently facilitated telemedicine capabilities by supporting open network communications.

Therefore, this research is concerned with hiding the patient's information and the medical image to increase security.

2.3 Information Security

Information security is the means of avoiding the entry, use, destruction, detection, disturbance, or disruption of data by intruders. It can be classified into two main categories: cryptography and hiding of information, which are the areas of research on information security that has existed for several years (Shaik et al., 2017), as shown in Figure 2.1.

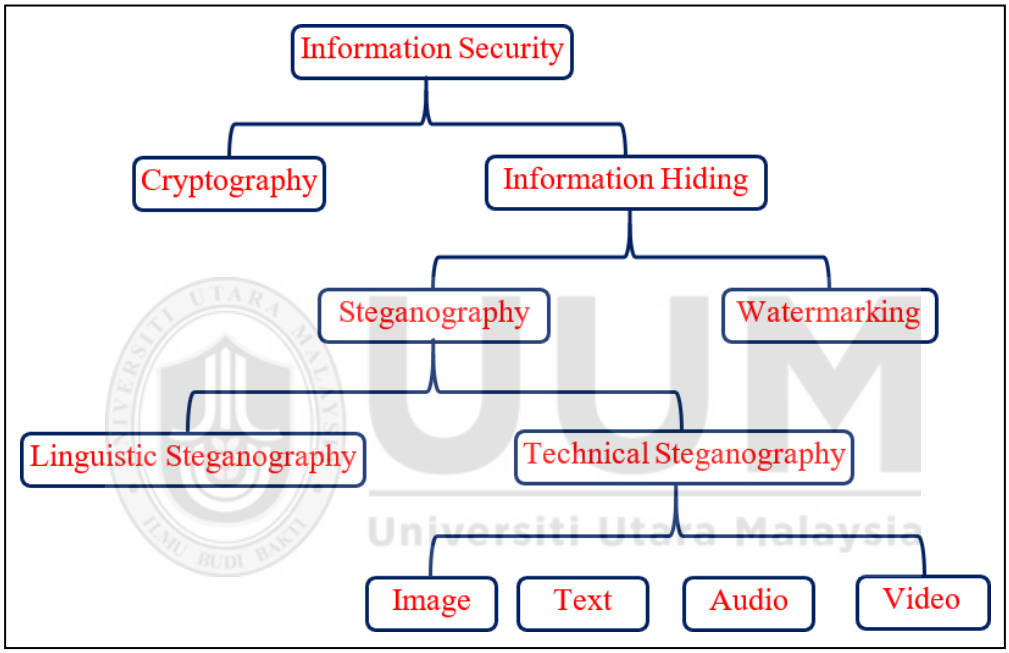


Figure 2.1 Information Security System (Subhedar & Mankar, 2014; Cheddad el at., 2010)

Cryptography and steganography are common ways of ensuring secure communication (Khaleel & Abduljaleel, 2021; Shawkat, 2016; Zhou et al., 2016). Cryptography is one of the most widely utilized techniques for maintaining data security. In contrast, steganography is the art and science of hiding information in a carrier, where nobody except the meant recipient knows the presence of hidden information. A significant development in data encryption technology has been achieved in recent years. Many approaches to data encryption are currently being used for digital image security. Random

encryption keys are made in these techniques, while genuine content becomes invisible (Hussain et al., 2018). Different security methods are used in digital communication, such as steganography and watermarking. These are the two essential sub-sections area of information hiding. Therefore, complete protection from unauthorized access or attacks on sensitive data communication is necessary.

2.3.1 Cryptography and Information Hiding

Cryptography and information hiding are both ways of protecting data against unauthorized users. Cryptography is primarily the study of converting information from its traditional form to an unreadable and incomprehensible format that is not understandable to anyone other than the intended sender and recipients. In other words, it encrypts the message to hide its meaning but not its existence. In contrast, information hiding hides and dissimulates the secret message in another cover carrier to suppress all proof that a secret message exists during communication. Information hiding maintains private communication between two parties (Abdel-Nabi & Al-Haj, 2017; Khalil, 2017; Al-Dmour & Al-Ani, 2015). Although cryptography and information hiding aims to provide secure communication, they have two declarations related to method breakdown. If the attacker can decode and read the secret message, it is cracked as a cryptographic scheme. On the other hand, if the hacker finds a hidden message, then a data shielding scheme is considered broken (Al-dmour, 2018). Table 2.1 shows a comparison summary between cryptography and information hiding.

Table 2.1

Comparison between Information Security Categories

		Information Hiding	
Criteria	**Cryptography**	**Watermarking**	**Steganography**
Objective	Data protection	Protect the carrier copyrights	Secure communication to prevent the leaking of secret messages
Carrier/medium	Text	Any form of digital medium (text, audio, image, and video)	Any form of digital medium (text, audio, image, and video)
Input Data	Plaintext	Watermark and cover carrier	Secret message and cover carrier
Output Data	Cipher-text	Watermarked carrier	Stego carrier
Key	Required	Optional	Optional
Type of Attack	Cryptanalysis	Image-processing operation	Steganalysis
Broken	If cipher-text is de-ciphered	If the watermark is removed	If the secret message is discovered
Challenge	Robustness	Robustness	Capacity and Imperceptibility
Reversible	Reversible	Reversible or irreversible	Reversible or irreversible
Extraction Type	Blind	Blind, non-Blind, and Semi-Blind	Blind
Visibility	Visible (conceal the meaning but not the presence of secret data)	Visible or Invisible	Invisible (hide the existence of confidential data)
Authentication	Full recovery of data	Usually achieved by cross-correlation	Full recovery of data
History	Oldest	Modern Era	Very olden except for its digital version

The above table summarises the differences and similarities between cryptography and information hiding are represented by watermarking and steganography according to several criteria, the most important of them (objective, carrier-medium, challenge, etc.) (Al-Dmour, 2018; Wazirali, 2016; Atawneh, 2015; Cheddad el at., 2010; Cheddad, 2009).

2.3.2 Steganography and Watermarking

Steganography and watermarking subjects fall under information hiding and are linked to a broader information security subject. They share specific properties, such as imperceptibility, capacity, and robustness, as in Figure 2.2. Nevertheless, their priorities and aims are different. For example, steganography safeguards the secret message that employs another carrier to provide concealed communication. Watermarking may be obvious and not inherently hidden because it is not meant to conserve confidential information but rather authenticate the origin of the tagged carrier (Cheddad et al., 2010). Regarding their priorities, steganography usually aims for imperceptibility (Tiwari & Shandilya, 2010), while watermarking goes for robustness (Hamid et al., 2012; Boato et al., 2009). In some cases, however, imperceptibility is not an issue for steganography, for example, when changing a specific carrier's color in the image. This adjustment may be undetectable; thus, the third party cannot access the original image (Hussein, 2020; Cox et al., 2008).

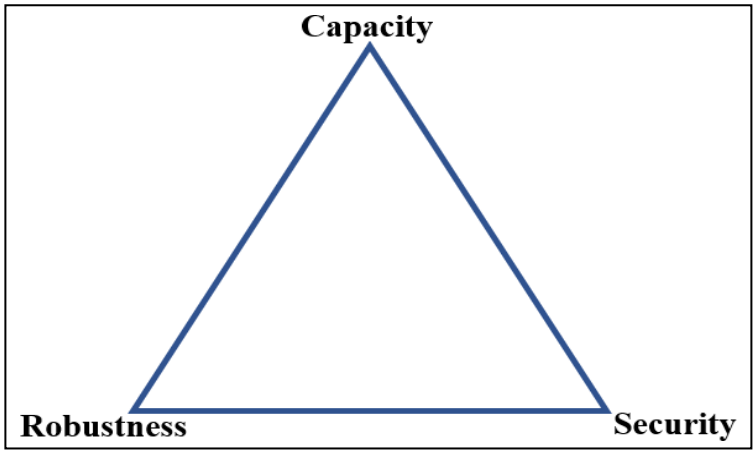


Figure 2.2 Information Hiding Properties (Mohamed, M. H., & Mohamed, L. M., 2016; Al-Ataby & Al-Naima, 2011)

Watermarking aims to embed information into the carrier medium that may be used to verify the authenticity and integrity of the carrier signal or to confirm the identification of its owners, as in watermarking of currency. Figure 2.3 is an example of using a watermark in financial currencies.

Figure 2.3 Watermarked Currency

Watermarking and fingerprinting are so close to each other. They mark carriers in the same method, except for watermarking; whole carriers have the same mark embedded for copyright preservation, while the carriers of fingerprinting are marked separately for each customer to prove ownership (Yu, 2016). Figure 2.4 shows the work of the information hiding with its two branches, watermarking and steganography.

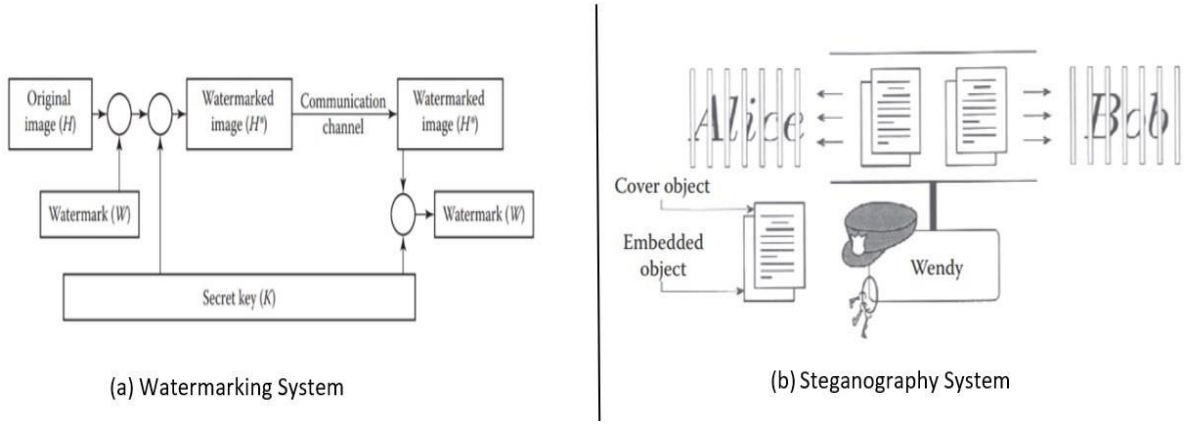


Figure 2.4 Information Hiding Branches (Shih, 2017)

Figure 2.4 (a) depicts a general digital watermarking scheme. A watermark W is embedded into a carrier message, defined as the cover image H. The image resulting from this is the watermarked image H*. A secret key K, a random number generator, is periodically involved in the embedding process to produce a more reliable watermark. On the other hand, the classic steganography scheme is described in Figure 2.4 (b); the warden Wendy observes all communications between Alice and Bob, so they must hide the messages in other innocuous-looking media (cover carrier) to obtain stego-objects. The stego-objects are then sent via public channels.

2.4 Steganography Systems

Steganography system security must fulfill Kerckhoff's principle, assuming that the attacker knows the system's design, the language used, and the algorithm for protection (Mahmoud & Elshoush, 2022; Khalind, 2015). Therefore, the security of a steganography system should depend on the stego-key to ensure that unauthorized users cannot retrieve the secret message without the stego-key. When the extraction process uses a stego-key

identical to the one used in the embedding process, this is referred to as a symmetric key. It is considered asymmetric if they are not similar (Saleh et al., 2016).

A typical steganography system consists of two primary phases: embedding and extraction. The embedding procedure involves inserting the secret message inside a host medium, such as a video, audio, or image file. The extraction procedure restores the embedded message from the cover. The extraction procedure is less complicated than the embedding procedure. The stego-key, which is needed to initiate the embedding or extraction process, is one method for enhancing steganography protection. Using the stego-key renders the extraction process computationally impossible for unauthorized users (Cheddad et al., 2010; Subhedar & Mankar, 2014).

In the study conducted by Vico (2010), the principle of a steganography framework is explained. The sender (Alice) sends a secret message (M) to the receiver (Bob) using a random cover medium (C). Alice can insert the message inside the cover medium using a stego-key (K). The resultant medium, also known as the stego-medium (S), should not be differentiated from the original medium (cover) to inhibit the hackers (Wendy) from retrieving the secret message. The stego-medium is transmitted to the recipient (Bob) over an insecure channel. The receiver then extracts the secret message since he is aware of the embedding process used by the sender and has the stego-key. Stego-key aims to create a secure steganography system. Wendy can observe the embedded message in the stego-medium and identify the embedding process, but the attacker cannot retrieve the embedded message without knowing about the stego-key. Accordingly, the stego-key should be as powerful as possible to block hackers from fracturing the steganography system using all possible stego-keys (Laskar & Hemachandran, 2012).

Computationally, the embedding process can be described as S = Em(C,M,K) and extracted as Mx = Ex(S, K). The extraction process ought to be reversible to the embedding process. Thus, Ex(Em(C,M,K),K) have to be equal to M (or Mx = M). Figure 2.5. shows a Schematic description of the Steganography Framework.

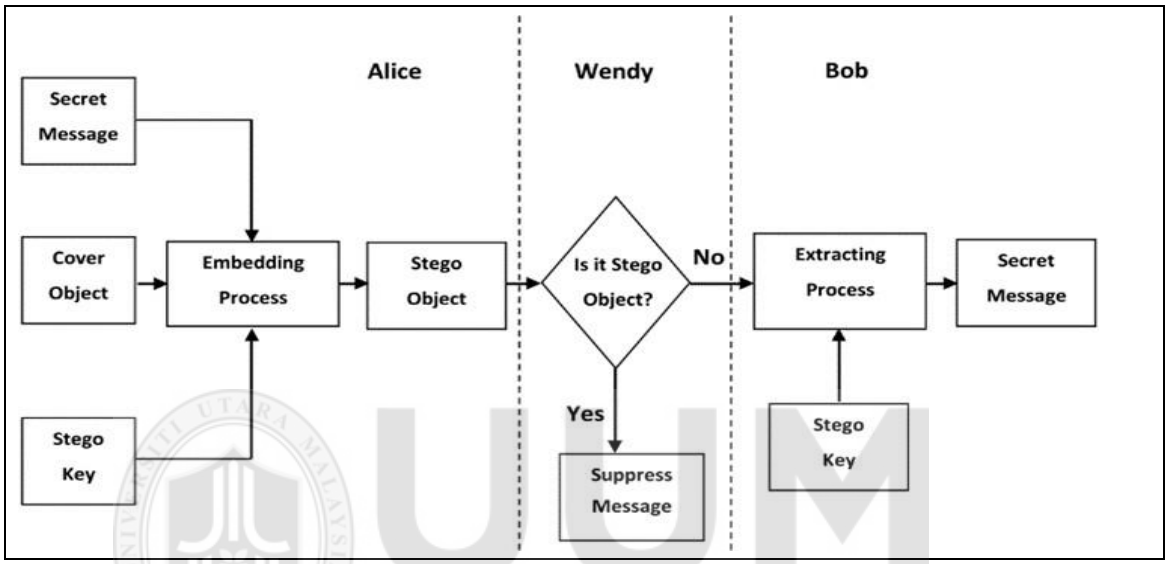


Figure 2.5 Schematic Description of Steganography Framework (Khalind, 2015)

It is evident from Figure 2.5 that the embedding process (Em) is the invert for the extraction process (Ex). The inputs of the embedding process are cover (C), secreted message (M), and stego-key (K), and the result of this process is stego-object (S). Simultaneously, the inputs of the extraction process are stego-object (S) and stego-key (K), which should transmit the same secret message (Mx), where Mx is the extracted secret message. The terminology of steganography is described below in Table 2.2.

Table 2.2

Definition Terms

	Terms Used	Definition
a)	Cover carrier (*C*)	The cover carrier is how the carrier conceals the secret message (M). Audio, video, image, and text are redundant carriers that can be used as cover carriers. Each cover carrier has a limited embedding capacity depending on the media type and the embedding method. The steganographer can select any cover carrier; contrast, a cover carrier for digital watermarking is restricted.
b)	Stego carrier (*S*) or Stego-medium	The stego carrier is the altered version of a cover carrier after successfully concealing a confidential message (Anandpara & Kothari, 2015). The cover and stego images should have a high degree of similarity, and the stego-carrier must at least preserve the imperceptibility feature to avoid a third party suspecting the existence of the confidential message (Hussein, 2020).
c)	Secret message (*M*)	A secret message points to the data concealed within the cover carrier. Confidential data can be any binary representation source that should be transmitted across an unreliable network without raising suspicion. In general, hiding more data increases the probability of detection, so selecting a proper cover is critical.
d)	Stego-key (*K*)	A stego-key can produce a robust hiding schema during the embedding and extraction. The key may be optionally used and generated using a pseudo-random number generator (PRNG) (Cox et al., 2008). Before communication starts, the key must be shared between the sender and the receiver; the extraction process is impossible without using the stego-key (Rashid, 2015).
e)	Embedding process (*Em*):	It refers to the process of concealing confidential messages in a cover carrier. There usually are three inputs: cover carrier, hidden message, and secret key (optional).
f)	Extraction process (*Ex*):	It refers to obtaining a confidential message from a stego-carrier by the authorized person. The extraction process is a reverse function of the embedding process; the inputs of the extraction process are the stego-carrier and secret-key, and the output is a confidential message.

2.5 Steganography Methods

Steganography methods divide as per their application in protecting cover files into four essential methods are cover type, embedding domain, embedding, and extraction approaches (Aparna & Kishore, 2018; Luo et al., 2008). Each method has different attributes and properties (El-Rahman, 2018; Muhammad et al., 2016). Figure 2.6 explains a graphical representation of the classification of steganography technical.

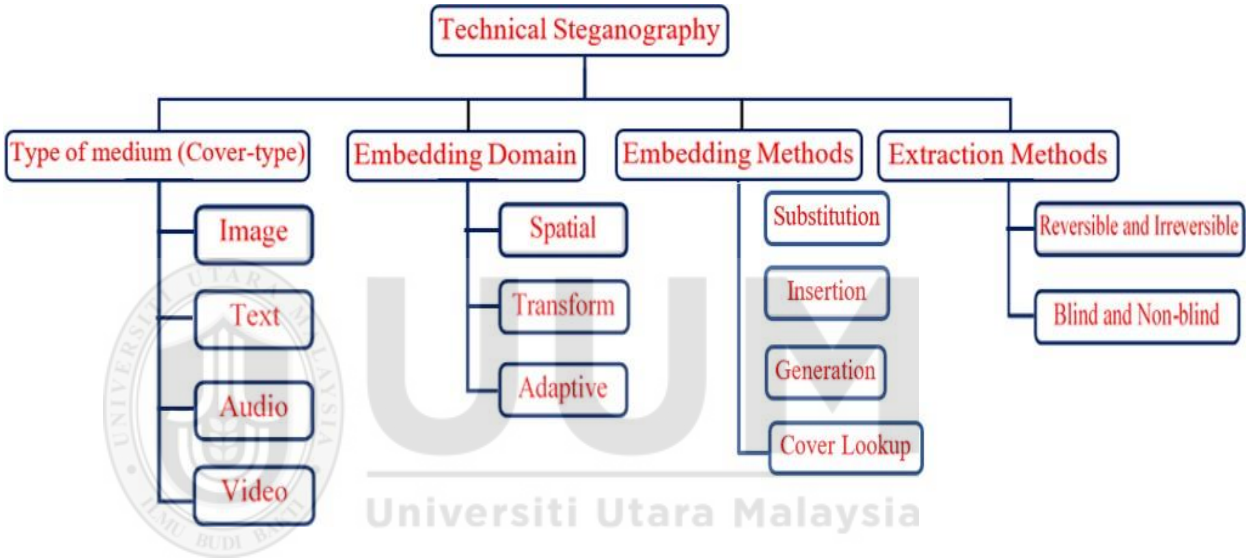


Figure 2.6 Schematic Description of Steganography Method (Al-dmour, 2018; Khalind, 2015; Rashid, 2015)

2.5.1 Types of Medium (Cover-Type)

Steganography techniques are divided into four digital types depending on the cover file format: image, text, audio, and video steganography (Hussain et al., 2018). If the image is utilized as a cover, it is called image steganography (Singh & Kaur, 2015). Similarly, if audio is used to hide secret messages, it is called audio steganography (Muhammad et al., 2015). Thus, several types of steganography are (i) Text Steganography, (ii) Image Steganography, (iii) Video Steganography (iv) Audio Steganography. Each cover media

has pros and cons (Dhar & Banerjee, 2019; Kadhim et al., 2019). Different file formats use different algorithms in steganography (Fadhil, 2016; Amirtharajan et al., 2010).

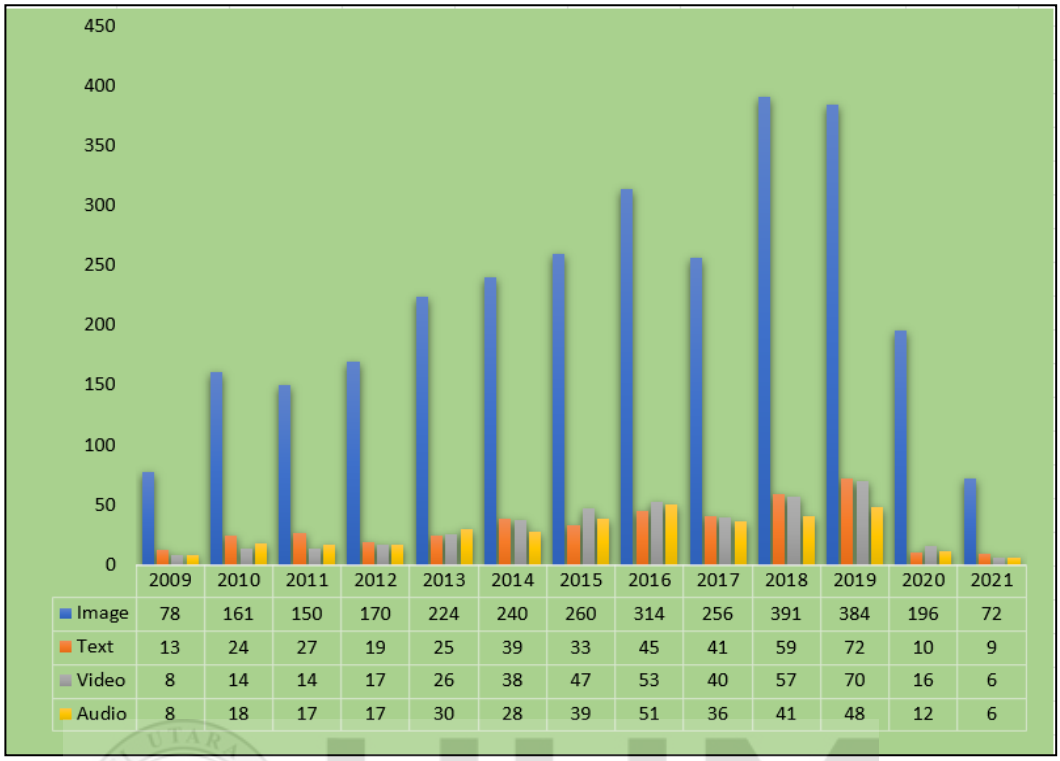
(i) **Text Steganography**: Text steganography, also known as linguistic steganography, is the most complex form because it employs natural written language to conceal a secret message (Johri et al., 2016; Chapman et al., 2001). The cover's content is created by changing the words or the design content. The cover content generated by this approach can meet all linguistic steganography requirements (Banerjee et al., 2013).

(ii) **Image Steganography:** It is perhaps the most prevalent form of steganography due to the vast inflow of electronic image data made available by digital cameras through the internet, high-speed delivery, ease of use by the users, and imperceptibility and large capacity (Subhedar & Mankar, 2020). Image steganography can conceal a secret message in the pixels of an image by embedding it as noise, which is nearly impossible for human eyes to distinguish (Mabrouk, 2017). Consequently, this research uses images as the cover medium to contain (conceal) the patient information as a secret message.

(iii) **Video Steganography:** A video file is used as the cover medium to conceal the secret message. Due to video files being composed of text, audio, and images, they are less susceptible to steganalysis. It combines frames that operate at a constant rate and are measured in f/s (i.e., frames per second). This approach works like image steganography, where it does alter the values of particular places in the images. Nevertheless, video steganography conceals confidential data in every video frame (Hossain & Parekh, 2016).

(iv) Audio Steganography: In this technique, the secret message is embedded within an audio file as the noise at frequencies beyond the range of human hearing; information hiding in audio files is incredibly challenging because of the sensitive nature of the Human Auditory System (HAS) (Djebbar et al., 2012). However, HAS still bears common modifications in tiny differential areas. For instance, high sounds tend to disguise quiet sounds. Furthermore, there are some typical peripheral deformations, so much so that listeners would ignore them. These features have led researchers to investigate audio signals as carriers to conceal data (Johri et al., 2016).

The statistics around the digital medium steganography have been obtained from Scopus and ScienceDirect. Figure 2.7 illustrates the numeral of steganography applications that conceal confidential messages in digital mediums from 2009 until 2021. The image ranked first among other digital media.



	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Image	78	161	150	170	224	240	260	314	256	391	384	196	72
Text	13	24	27	19	25	39	33	45	41	59	72	10	9
Video	8	14	14	17	26	38	47	53	40	57	70	16	6
Audio	8	18	17	17	30	28	39	51	36	41	48	12	6

Figure 2.7 The Cover Files Used in the Steganography Applications

An image is the most common cover medium for embedding secret data. Because of the high degree of redundancy and prevalent use in a computer environment and easily shared on the World Wide Web (WWW) will not raise any suspicion (Nabi & Afzal, 2020; Pradhan et al., 2016; Tiwari & Shandilya, 2010).

2.5.2 Embedding Domain

Based on the domain used by the embedding technique, steganography techniques have been classified as (i) spatial domain, (ii) frequency (transform) domain, and (iii) adaptive (Nipanikar & Deepthi, 2019; Muhammad et al., 2015; Banerjee et al., 2013; Pevný et al., 2010). The frequency domain is also called the transform domain (Kumar, V. & Kumar, D., 2018; Cho et al., 2013; Prabakaran & Bhavani, 2012; Wu et al., 2009; Fridrich et al., 2007). Spatial domain algorithms modify the carrier pixel value directly to add a secret

message like the LSB technique (Shah & Bichkar, 2019; Abdullah & Hussein, 2020). At the same time, in the transform domain, modulation is done on the transform coefficients of the cover carrier. Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), and Discrete Cosine Transform (DCT) are examples of transform-domain techniques.

Present steganography techniques are the spatial and the transform domains. Many algorithms and methods, such as the LSB, and Pixel Value Differencing (PVD), utilize the spatial domain (Anandpara & Kothari, 2015). Before embedding, it is essential to identify the zones or data that changed without compromising the cover file (Kanan & Nazeri, 2014).

(1) ***Least Significant Bit (LSB) Technique*:** LSB is one of the most popular, easy-to-use methods for obscuring data in a cover medium (Shah & Bichkar, 2019; Hussain et al., 2018). More details about the LSB technique will present in section 2.6.

(2) ***Pixel Value Differencing* (PVD):** This scheme divides a cover image into blocks so that the split blocks are not overlapped. The pixel difference in a pair of blocks is utilized to conceal confidential data (Shukla et al., 2018; Hong et al., 2012).

(3) ***Grey Level Modification* (GLM)**: Steganography of the spatial domain image is also used for mapping data. Images are usually represented in pixel levels of grey or intensity. These grey levels are used for embedding messages in this sketch. First, a pixel's intensity or grey level is taken in the image. This value is then matched to the secret message's bit values to be hidden (Hashim et al., 2018; Shelke & Jagtap, 2015).

(4) ***Parity Checker Method*** **(PCM):** Parity values are used in the PCM diagram. This method utilizes two forms of parity (even and odd). The one value is placed at the site of pixels to consider pixels to have parity even. Similarly, the zero is replaced at that pixel site to identify the pixel, which must be odd parity (Shelke & Jagtap, 2015; Gayathri & Kalpana, 2013).

(5) ***Exploiting Modification Direction*** **(EMD)**: This way, pixel pairs conceal messages within the host image. It has a limited number of hiding information notation systems. However, adjustments are made in one pixel only. The capacity of this scheme is greatly improved (Qin et al., 2015).

(6) ***Diamond Encoding*** **(DE):** The pixel pair is utilized in this form of steganography; this improves the capacity for data storage compared to EMD. It provides robustness for transmissions through the unsecured channel to the communication system (Hong et al., 2012; Chao et al., 2009). The effect of image degradation is reduced after hiding information.

(7) ***Optimal Pixel Adjustment Process*** **(OPAP):** This technique gives the image's desired look. It sets the pixel values for purposes of data hiding. It is like the LSB substitution technique. After information hiding, the stego-image is very close to the host image before hiding the secret data (Kaur & Goel, 2015).

Table 2.3 shows spatial domain schemes' comparative advantages and disadvantages.

Table 2.3

Spatial Domain Schemes

Technique	Advantages	Disadvantages
LSB	- It is simple to understand. - Easy implementation. - Good payload capacity. - The resultant Stego-file will be similar to the cover file after embedding secret information.	- Get cracked by a third party (unauthorized user). - Increased embedding capacity negatively affects the quality of the cover file.
PVD	- The image quality is maintained. - High embedding capacity	- The complexity level is very high. - Weak defense against geometric attacks, compression, and statistics.
GLM	- The complexity level is less than PVD.	- The data sometimes get lost.
PCM	- A simple mechanism is used for two parity (even and odd). One for even and zero for odd. - It can retrieve message bits from all locations.	- Data storing capacity is low.
EMD	- High security for the transmission of secret messages.	- Data storing capacity is larger than PCM, but the maximum value is (1.61-bit per pixel)
DE	- High capacity.	- This modification process introduces extra distortion to the stego-image.
OPAP	- Improved quality of the image.	- The little amount of distortion after information hiding.

Depending on steganography techniques, many researchers worked to hide information using different methods like LSB substitution, LSBM, PVD, edge detection filter, adaptive LSB and pixel indicator techniques, and texture-based techniques.

Samidha and Agrawal (2013) suggested applying new techniques with the LSB hiding algorithm in the spatial domain. Random pixels are selected to hide a secret message in any sequence from (LSB to MSB) location. Several parameters have been considered,

such as pixel color and physical location. A new adaptive LSB steganography using PVD was suggested by (Yang et al., 2008). The pixels in edge areas add more bits of a secret message than smooth regions. The suggested approach provides more significant potential for embedding and better image quality than PVD and LSBR. New steganography has been proposed using the GA to preserve the character of the statistics (Wang et al., 2010). The method includes embedding the cover image's secret message in LSB and allowing GA to change the stego-image to preserve its statistic characters. The approach was designed to resist the Reversible Statistical (RS), where the experiment results showed a good balance between security and image quality. Wu, Kao, and Hwang (2011) suggested a new secret image-sharing schema using the optimal pixel adjustment operation to improve image quality under different payload capacities and authentication bits. The results mention that the proposed method achieved high visual image quality and stego-image authentication capability. Ullagaddi, Cameron, Hassan, and Nims (2013) suggested covering classified data in images according to three various levels of security. The pixels are randomly selected, and the higher nibble bits match the data bits. A two-bit code (2BC) is created to encode the site of the matching bits. The researchers suggested three techniques to integrate the 2BC into the image. Although the LSB technique is vulnerable and limited to rotation, low-bit reverse, compression, and cropping attack, the method is tough to intercept.

Modi, Islam, and Gupta (2013) developed a color image steganography using the Canny edge detection method and LSBM to hide 2-LSBs of edge pixels. Only one stream (R, G, or B) applies the Canny rule. Then the pixels are chosen to be inserted in the other two channels corresponding to the edge pixels. This method's primary limitation is the low

embedding capacity (payload), where the capacity is 0.083 bpp of the color image's edge pixel. It is also not possible to use this method for grayscale images. It exploits the edges of the medical image from the diagnostic area in embedding information because the human visual system (HVS) is less sensitive to high disparity areas than its smooth areas (Al-Dmour et al., 2015). The experiment results showed that the proposed technique offers a high payload and better stego-image quality. By utilizing the decision tree, the medical image steganography method securely transmits the patient data within a medical image with the RSA encryption algorithm. It hides the secret blocks in the LSB of the cover image through a breadth-first search-based mapping mechanism. However, it is suitable only for mapping a small amount of confidential information and medical images (Jain et al., 2016). A developed RGB image steganographic technique is suggested for secure communication (Mondal et al., 2016). The image steganography approach exploits the Swapped Huffman tree encoding to encrypt the medical data and generate the stego images with higher quality and imperceptibility (Usman, M. A. & Usman, M. R., 2018). Table 2.4 briefly lists the associated works in the spatial domain and their strengths and weaknesses.

Table 2.4

Spatial Domain Techniques in Image Steganography

Author	Method	Strength	Weakness
Yang et al. (2008)	- Adaptive Least Significant Bit (ALSB) – PVD	Large embedding capacity and high quality	This method is not tested against relative attacks
Wang et al. (2010)	LSB and GA	The efficiency in resistance against steganalysis with better quality	Easy statistical detection of artistic effects
Wu et al. (2011)	Optimal Pixel Adjustment (OPA)	A good result in imperceptibility and capacity	Security against steganalysis attacks not approved
Modi et al. (2013)	LSBM, Canny edge detection	High robustness, robust against visual attacks	This method has many limitations: low capacity, cannot use with grayscale images
Ullagaddi et al. (2013)	- Two-bit code (2BC), LSB	Very hard to intercept	Limited to compression, cropping, rotating, and low-bit reverse attack due to LSB weakness
Al-Dmour and Al-Ani (2015)	- LSB, Edge Detection. - Hamming code	High payload and good quality	No consideration to increase security with cryptography
Mondal et al. (2016)	- Plane Bit Substitution Method (PBSM) and LSB	High capacity with a better peak signal-to-noise ratio (PSNR)	Suffer from spatial domain limitation
Jain et al.2016)	- LSB's substitutions with Decision Tree, RSA algorithm	Best capacity**.**	The complexity of the encryption is very high.
Usman and Usman (2018)	- LSB, Swapped Huffman Tree coding (SHT), Canny Edge.	- Ensures confidentiality - Maintaining imperceptibility.	The capacity of this method is dependent on the number of edge pixels that are detected.

2.5.3 Embedding Methods

Steganography can be categorized according to the technique used to hide confidential data, regardless of the cover used to conceal information. There are four ways of hiding confidential data in cover files; i) insertion-based method, ii) replacement-based method, iii) generation-based method, and iv) cover-based lookup method. (Atawneh et al., 2013; Cox et al., 2008; Kipper, 2004).

(i) Substitution-Based Method: This method differs from the insertion-based method; no hidden message is applied to the cover carrier information by the substitution-based process. Nevertheless, the alternative method identifies irrelevant regions or information in the cover carrier and replaces it with a secret message. Therefore, the dimensions of the stego and the cover files are identical since some of the cover information is changed and replaced without additional data. However, after the embedding process, the quality of the cover carrier can be destroyed. In addition, the limited amount of unimportant information in the cover carriers limits the size of secret information that can be concealed (Al-Afandy et al., 2016; Kipper, 2004). There are three ways to select the embedding positions:

(1) **Sequential selection:** The cover elements are modified individually and consecutively to embed the confidential message. This method is easy and simple to implement. However, it has a high probability of detection (Khalind & Aziz, 2014).

(2) **Random selection:** The embedding locations are selected randomly. The receiver and sender must utilize a secret key to generate the same random number subset. A pseudo-random number generator (PRNG) has a higher security level than a sequential selection (Sharif et al., 2017).

(3) **Adaptive selection:** The adaptive selection rule chooses the cover elements for embedding based on their features. For example, the edge detection method can be applied to the cover image to select the high-contrast regions for embedding, which are less detectable than the smooth regions. In terms of detectability, adaptive selection achieves a better security level than sequential and random selection methods (Kumar et al., 2019).

(ii) Insertion-Based Method: The file-reading software generally ignores several zones in cover files, so the insertion-based steganography method adds the secret message within cover areas. This approach thus retains readable regions without change, which benefits this type of embedding. Accordingly, confidential data could be added to any cover file without restricting the embedding capacity. However, the size of the stego file would be much greater than the cover file size due to adding the secret message to the cover file without deleting any portion of it (Al-Afandy et al., 2016). Sometimes this size difference can make the stego-file suspicious without looking at the data content. A good example of that method is to insert a confidential message between a Word document's end-text and start-text signs in the field.

(iii) Generation-Based Method: Generation-based approach to steganography or cover synthesis is unlike all insertion and substitution-based methods in terms of the presence of the cover carrier as it produces correct stego carriers using secret messages (Cox et al., 2008). The cover carrier does not exist; only stego carriers are available. Therefore, one benefit of generation-based steganography is that detection technique that depends on comparing stego with the cover carrier are prevented. However, the main limitation of this approach is the restricted stego files that can be created. Also, it can produce

unrealistic files, such as images with lots of random colors and shapes that do not contain meaningful information or create text without meaning that can alert attackers to the presence of the secret message (Khalind, 2015).

(iv) Cover lookup-based method: This method searches for a pre-existing cover carrier to be used as a secret data container, so there is no need to alter anything in the cover carrier to hide secret data (Obaid, 2015). It supposes that the convenient cover carrier that already contains the desired secret message can be found. This method becomes impractical when the size of the secret message increases.

2.5.4 Extraction Methods

Steganography systems can be divided into two categories based on extraction: i) reversible and irreversible and ii) blind and non-blind.

(i) Reversible and Irreversible Types

Reversible steganography techniques are employed to restore the original image in addition to confidential data from the stego image. This type is essential in medical diagnosis, military, and remote-sensing applications, where retrieving the cover image has the same priority as retrieving the secret message. In contrast, irreversible methods are only concerned with recovering the secret message (Kumar & Muttoo, 2013; Hong et al., 2011).

(ii) Blind and Non-Blind Types

Steganography methods can be classified into blind and non-blind based on the requirements of the extraction process (Cox et al., 2008).

(1) **Blind Steganography:** Usually, steganographers suppose the cover carrier is unnecessary for the extraction process because the receiver does not require it. Hence, the cover carrier is disregarded, and the sender can use any medium for embedding the secret data.

(2) **Non-Blind Steganography:** The non-blind steganography method cannot be applied without the existence of the original cover. The original cover plays an essential role in extracting the secret data in the non-blind method, and the recovery of concealed information would be unattainable without it.

2.6 Least Significant Bit (LSB) Technique

LSB is one of the most prevalent, simple, and straightforward techniques for concealing information in a cover medium (Shanthakumari et al., 2021; Hussain et al., 2018). This technique has a minor effect on the cover medium, and the naked eyes would undetectable it. The LSB values are modified directly from the cover's pixels to embed the message into the image, which is used as a host (Hussein, 2020; Mohamed, 2018; Collins & Agaian, 2014; Gayathri & Kalpana, 2013). The resulting image (i.e., stego-image) is indistinguishable from the host image due to its high quality, but it suffers from weak resistance to attackers. Therefore, many researchers worked to develop this technique and end LSB-steganography problems by providing other solutions, using many k-LSB bits in the bitplane levels to achieve more capacity and security. Table 2.5 summarizes several studies related to k-LSBs steganography regarding pros and cons.

Table 2.5

Studies Related to k-LSBs Steganography

References	No. of LSBs	Pros	Cons	Notes
Wang et al. (2001)	k-LSBs, where k denotes the number of LSBs of the host image' pixels utilized to store the secret message bits.	Improve the Quality	The robustness is not considered.	There is a trade-off between the amount of embedded data and the quality of the resulting image.
Chan & Cheng (2004)	4LSB means 1st, 2nd, 3rd, and 4th LSBs.	Increased capacity	Image quality degraded drastically as the bit level increases	When k>=4, the quality of the resulting image degrades dramatically.
Ahuja & Kaur (2009)	Use 4 LSBs of each RGB (Red, Green, and Blue)	Providing high capacity	The quality is not considered.	
Zeki & Manaf (2009)	Intermediate significant bit (ISB)	Improve the robustness and maintain the quality	Capacity not addressed	A GA is used to find the best intermediate bit out of the bitplanes.
Pharwaha (2010).	Confidential data was inserted in the first three LSB positions per pixel.	Improved security only	Quality not addressed	Confidential data is embedded in the first three LSB positions in the pixel while avoiding the pixel value is 111 in the three LSBs.
Bamatraf et al. (2010)	Used the 3rd and 4th LSB bits.	Improved security and quality	Capacity did not address	

References	No. of LSBs	Pros	Cons	Notes
Swain & Lenka (2012)	Used 1-LSB, 2-LSB, 3-LSB, and 4-LSB, which are in locations 8^{th}, 7^{th}, 6^{th}, and 5^{th} of bit-planes	An enhanced Security and Capacity	Robustness did not consider	
Gutte et al. (2013)	2LSB or 3LSB for comparison.	Maintain the quality for both 2LSBs and 3LSBs.	Capacity did not consider	The difference between the PSNR for each of the data was slight.
Kanan & Nazeri (2014)	LSB	Enhanced quality	Robustness did not address.	A GA is used to find a starting position and direction.
Mohammed (2015)	Dual Intermediate Significant Bits (DISB) technique.	An enhance the quality and robustness	Capacity did not consider	Finding the best two intermediate bits out of the bit levels by GA.
Khan et al. (2015)	Use 4 bits LSBs from the edges of the cover image.	Increase the stego-image quality and security.	Decreases the hiding capacity	Used canny-edge detection to find valid edge pixels.
Bharti et al. (2017)	Use 4 LSB bits for comparison.	Improve quality and capacity	Robustness did not consider	Quality is inversely proportional to image-hiding capacity.
Sari & Siahaan (2018)	Used 1,2 LSB. The pixel sequence is an RGBRGBRG for 1-bit and RGBR for 2-bits.	Improve quality	Robustness and security did not consider.	1-bit LSB is much better than 2-bit.
Shah & Bichkar (2019)	LSB	Achieved high payload capacity	imperceptibility did not consider.	A GA is used to find a starting position, direction, and polarity.

The literature also contains medical image steganography methods based on LSB. The LSB technique was utilized due to its attractive characteristics, ease of understanding, and application to meet specific information steganography requirements, such as imperceptibility, capacity, and security. Table 2.6 summarizes these works and lists their most significant characteristics regarding embedding regions, the number of bits used, and performance metrics. These include works (Lavanya and Natarajan, 2012), (Pai et al., 2012), (Thiyagarajan and Aghila, 2013) (Liu et al., 2016), (Mantos and Maglogiannis, 2016), (Jain and Kumar, 2017), (Arunkumar et al., 2018), (Salameh, 2019), (Ogundokun et al., 2020), (Subhaluxmi Sahoo and Sony Snigdha Sahoo, 2020), (Karawia, 2021), and (Priyadharshini et al., 2021).

Table 2.6

Medical Image Steganography based on the LSB Technique

References	Encryption	ROI Decomp.	Non-Contagious	Bit-Plane	Performance Metrics	Limitations
Lavanya and Natarajan, 2012	√	×	×	1 bit	Normalized cross-correlation (NCC), Root Mean Square Difference (RMSD), and Average Difference (AD).	Combining both spatial and frequency domains.
Pai et al., 2012	×	√	×	1 bit (Simple LSB)	PSNR	Increasing capacity, which is non-determined, negatively affects the quality
Thiyagarajan and Aghila, 2013	×	√	×	Non-determined	PSNR. MSE and Bit error rate (BER)	Only used the Non-Region of Interest (NROI) as an embedding area.
Liu et al., 2016	√	√	×	3 bits	PSNR	Lacking the support of non-contagious message embedding.
Mantos and Maglogiannis, 2016	√	√	×	1 bit	PSNR	Only used the smooth region as an embedding area.

References	Encryption	ROI Decomp.	Non-Contagious	Bit-Plane	Performance Metrics	Limitations
Jain and Kumar, 2017	√	×	×	4 bits	PSNR, MSE	The computational time of the encryption system is very high.
Arunkumar et al., 2018	√	×	×	Non-determined	Histogram	- The increasing size of the host image. - Contagious region affects security.
Salameh, 2019	√	×	×	Non-determined	PSNR, MSE	High-cost computational due to combining cryptography and steganography techniques.
Ogundokun et al., 2020	×	×	×	1 bit	PSNR. MSE and SSIM	Compared with the existing systems.
Subhaluxmi Sahoo and Sony Snigdha Sahoo, 2020	√	×	×	1 bit	NCC, RMSD, and AD	Combining both spatial and frequency domains.
Karawia, 2021	√	×	×	4 bits	PSNR, MSE, Histogram, and Chi-square	Increasing the number of variable bits increases the embedding payload, negatively affecting image quality.
Priyadharshini et al., 2021	√	×	×	1 bit	PSNR, MSE	Comparison of encrypted and unencrypted image steganography results utilizing LSB without encoding.

2.7 Image Steganography

Image steganography points to hiding secret messages in digital images with the intention of secret communication between communicating parties to avoid the suspicion of non-communicating parties, to attacks and eavesdropping on this kind of communication (Raghu et al., 2021). For example, military communications and medical systems pass sensitive information over public networks where anyone can access and connect to the internet (Shibani et al., 2020). The distribution and maintenance of medical records in the digital medical system are necessary. For example, during orthopedic surgery, it may be required to send the patient's details and medical images to a pathologist and radiologist, which requires maintaining this information to protect the privacy of the patient's details. The main purpose of using technical steganography for medical images is to increase the security, integrity, and confidentiality of patients' data records and medical images. Medical image steganography is considered a particular state where medical images have unique demands (Singh, 2015). In modern health care, exchanging medical information between hospitals/clinics has become a daily routine. Medical image steganography is employed to protect the EPR's confidentiality without affecting the quality of the medical image. It conceals the EPR and diagnosis report in their medical image to solve the authentication issue and preserve patient privacy by linking the patient's information and their image (Al-Haj, 2015; Nyeem et al., 2013).

Over recent years, more attention has been paid to improving the safety of patient information in medical databases by considering steganography schemes as a solution for covering EPR in photographs of patients. This interest has arisen within several techniques of steganography that are designed to fit the requirements of medical images. Methods of

steganography are employed in the health care system for many causes, including (Karmakar & Basu, 2019; Dagadu & Li, 2018):

(a) Privacy and Confidentiality: Data privacy is essential since patient images and data are shared between hospitals via unsecured public networks. The steganography scheme prevents hackers from becoming aware of communication channels. Additionally, it safeguards digital medical images and sensitive patient data during transmission.

(b) Security: The major feature of steganography is the inability of intruders to discover the message statistically. More precisely, steganography's security is determined by supposing that the intruder cannot prove whether the cover medium contains confidential data.

(c)Saving Power and Cost: Computational and memory costs are necessary criteria for evaluating an information system. Since medical system databases typically have many data to carry, it is fair to use methods that preserve the essential data but require a minimum memory. The needed storage for patient records can be minimized in the Medical Information System (MIS) by hiding EPR inside the medical image. However, the computational cost of information-hiding methods should be appropriately compared to other information security methods.

(d) Availability: Availability is the capability to guarantee authorized users have access to the information system and resources related to the information system at any time authorized.

In this research, since the image is chosen as a cover in the embedding process, a simplified explanation of the format of the digital images, segmentation methods, and optimization techniques are included as follows:

2.7.1 Format of Image

The digital image is a numerical representation, typically as a series of ones and zeros (also known as binary). In the 2-D image f(x,y), each site represents a point, or what is known as (a pixel), which is the smallest unit to describe a specific location on the screen (Wu et al., 2015). Every pixel is expressed in a limited number of bits by an actual number or a series of real numbers. The more these units (Pixel) increase within fixed limits, the greater the convergence of this image of the human eye's reality to this image sensor's facts, called (Resolution) (Younis et al., 2016). Every pixel plane-bits deepness into the present color schemes is 8. The 8 bits are used to describe each pixel's color. Monochrome or grayscale images use 8 bits per pixel and present 256 (2^8) colors or grey shades (Ramakrishnan, 2018). Digital color images are mainly kept in 24-bit formats, using the RGB color pattern, called an actual color. A 24-bit image's pixel colors are based on three primary colors, red (R), green (G), and blue (B), where 8 bits are used to represent each base color. Each pixel has 256 different red, green, and blue colors, totaling more than 16 million (Tiwari & Shandilya, 2010). A pixel with 255 green and 0 red and blue values renders the color green. A 24-bit image with 1024 × 768 resolution contains around 2.36 MB of data.

Embedding any text or digital image in a digital image is possible. When a secret message is concealed inside an image, the pixels of the image are modified and inserted based on confidential data (Lin, 2011). A common characteristic of most images is that neighboring pixels are correlated, and redundant information exists. Redundancy is deemed the carrier bits that offer the topmost accuracy for the carrier's presentation; this involves the bits that can be modified without losing the image's integrity. Most digital formats are suitable for

steganography; nonetheless, those with greater levels of redundancy are more appropriate, like video. The main thing to remember in a cover image file format is that there is not just a single image type; there are many. Each image type has pros and cons, which must be considered to use the correct type.

Image steganography can be performed using raster or vector cover images. The LSB is the essential type of raster steganography, which hides the message in the cover image's LSBs. The changes are slight; they are invisible to the naked eye. In contrast, vector image steganography methods can be split into jittering and embedding (Madoš et al., 2014). Jittering is like LSB steganography because of storing the secret message in the least significant digits of point coordinates in vector images. Below are the most common image formats for using them in the web and computer graphics:

(i) Raster Image: A raster graphics or a bitmap image is a set of bits that determine the color of each pixel in a rectangular pixel grid (color dots), which can be viewed via a screen, paper, or another display media. This image is stored in various formats such as JPEG, BMP, GIF, and PNG (Almutairi, 2018).

(ii) Vector Image: Vector graphics are the construction of digital images through a series of mathematical expressions placing lines and shapes in an offered 2-D or 3-D space; Portable Document Format (PDF), Adobe Illustrator (AI), and Encapsulated Postscript (EPS) are examples of vector file format (Madoš et al., 2018).

The main difference between these entire image formats depends on 1) compression and 2) compatibility. Table 2.7 describes each type of image format, including its advantages, disadvantages, and applications.

Table 2.7

Description of Various Image Formats

Image-Type	Image Format	Advantage	Disadvantage	Application
Raster image	JPEG/JPG (Joint Photographer Expert Group) (Sinha, 2015; Fridrich et al., 2002)	- Most commonly used image types for small sizes. - Allows users to specify the compression level	- Low image quality at higher degrees of compression	- Images for on-screen display (websites and PowerPoint representation)
	GIF (Graphic Interchange Format) (Elgabar & Alamin, 2013).	- The lossless format supports both animated and static images. - Good for webpage banner ads.	- Large file size. - Limited color support (256 colors or 256 shades of grey).	- Images for display on a website.
	PNG (Portable Network Graphics) (Almutairi, 2018; Oktavianto et al., 2017).	- Best of lossless image formats. - Good image quality. - Widely supported across the web. - Support 16-bit (Grayscale) or 48-bit (true color)	- Limited acceptance with an earlier web browser.	- Teaching files; images for display on a website; publications
	BMP (Elgabar & Alamin, 2013; Eltyeb & bed Elgabar, 2013).	- They offer little to no compression, which results in unnecessarily large files.	- Large file size.	- The BMP images are widely used on Windows operating systems and other platforms.

Image-Type	Image Format	Advantage	Disadvantage	Application
Vector Image	TIFF/TIF (Tagged Image File Format) (Ansari et al., 2019)	- Offers both compressed and uncompressed versions. Compressed is similar to PNG, and uncompressed is similar to BMP.	- Large file size.	- Format preferred by journals for publication
	PDF (Portable Document Format)	- The most widely used document format. - To print documents as an image.	- The file size is large, depending on the document's content.	- To print documents as an image.
	EPS (Encapsulated PostScript)	- EPS is a file extension for a graphics file format. - Standard format for the print industry. An EPS file can contain text as well as graphics.	- Any modification of an EPS file's text, line, or color is not supported by graphic design programs.	- EPS is used for printing to PostScript printers and imagesetters, and it is the best choice of graphics format for high-resolution printing of illustrations.
DICOM	Digital Imaging and Communications in Medicine	DICOM is most commonly used for storing and transmitting medical images	- The possibility to enter many optional fields, some of which may be empty of data	- Telemedicine

2.7.2 Segmentation of Image

Image segmentation is splitting an image into various parts, regions, or sets of pixels with similar attributes (Abdulateef et al., 2020; Nikolic et al., 2016). It is referred to as one of the essential image-processing processes. It is helpful for applications like carrier recognition or image compression because it is not good to process the whole image. This processing may affect essential parts of the image, as in the medical image. The medical image includes the region of interest (ROI) and non-interest (RONI). To separate them, the medical image undergoes a segmentation process; image segmentation is a procedure for extracting the most significant portion of a medical image, the ROI. This region contains the worthiest data in the medical image and should not undergo modification. The medical image can have many ROIs areas (Aparna & Kishore, 2018; Norouzi et al., 2014). Since all regions of interest (ROIs) are significant in the medical image, segmenting a medical image requires a specialized medical expert. Generally, the techniques of medical image segmentation can be classified into three groups based on the level of human interaction (i) manually, (ii) semi-automatic, and (iii) fully automatic.

(i) Manual Segmentation: By the human expert (i.e., expert physician), the boundaries of the objects and areas of interest are identified and defined by them using their prior knowledge and experience as well as the information presented in the image to get a more precise segmentation result (Al-Dmour, 2018; Foster et al., 2014). In this method, the human expert uses custom software tools with advanced graphical user interfaces (GUI) to ease the identification of regions of interest and image display (Gordillo et al., 2013). However, manual segmentation is considered the most precise because of the difficulty of precisely and reliably drawing structures in medical images. In other

words, the quality of the image and its artifacts determine segmentation difficulties (Despotović et al., 2015).

(ii) Semi-Automated: This method is a middle between manual and completely automated segmentation methods, as it relies on two factors: the human aspect (i.e., the expert physician) and his sharing of computer programs (Fawzi et al., 2021; Lim & Mandava 2018). The specialist physician inserts some parameters, checks the efficiency of the outcome, and manually adjusts the segmentation result. The other factor (i.e., computer programs) implements what was directed to the computer by converting the input parameters to the program and outputting the result in visual comments subject to the expert's evaluation, which provides feedback for the processing (Sun, 2019). This approach is practical when no automatic method leads to optimal segmentation (Yushkevich et al., 2016).

(iii) Fully Automated: It is the use of computer programs to segment the images without the intervention of the human factor, as there are no input parameters and no directions by the user; only his task is to provide the computer with the images to segment (Wadhwa et al., 2019; Gordillo et al., 2013), it means the performance of automatic approaches is purely dependent on the knowledge bases, even in the absence of specialists (Chahal et al., 2020). This method is fast and good in some situations. However, it is still challenging to solve all segmentation problems by automatic segmentation algorithms because each method has positive and negative features (Hameurlaine & Moussaoui, 2019). Because of the contrast and complexity of the image, there is no single technique that can be considered suitable for all types of

images, and not all methods are equally suitable for a particular type of image (Abdulateef & Salman, 2021; Agrawal & Tyagi, 2020; Jeevitha et al., 2020).

2.7.3 Optimization Technique

AI generally refers to computational tools that can substitute for human intelligence in performing specific tasks. In computer science, an ideal "intelligent" machine is a flexible rational agent that perceives its environment and takes actions that maximize its chance of success at some goals. In other words, the term "artificial intelligence" is applied when a machine mimics "cognitive" functions that humans associate with other human minds, such as "learning" and "problem-solving" (Sadiku et al., 2021). Recently, there has been a significant increment in using AI techniques in image processing to enhance solutions. Medical image processing includes compression and segmentation (Jagadeesh & Rajendran, 2019).

The medical image processing process is one of the most critical research areas in the digitized medical information field because of the important challenges in sharing medical information through unsecured channels (internet), which requires protection from attackers (Al-Rababah & Al-Marghirani, 2016). Finding a solution to a problem with limited information under uncertainty in computer science and artificial intelligence is often called the method of searching through space for feasible solutions (Bianchi et al., 2009). On the other hand, optimization finds the best solution among available solutions (Agarwal & Mehta, 2018; Dhiman & Kaur, 2018). Common AI algorithms used for optimization are Swarm Intelligence (i.e., Ant Colony Optimization, Artificial Bee

Colony, Practical Swarm Optimization, and Harmony search) and Genetic Algorithm (Phonsa & Bansal, 2018; Pham & Castellani, 2014).

The literature contains a considerable amount of research on using meta-heuristic searching to optimize the process of steganography (Snasel et al., 2020; Wazirali et al., 2019; Hemanth et al., 2016; Roy & Laha, 2015). Various type of meta-heuristic searching algorithms was used; evolutionary genetic approaches (Shah & Bichkar, 2021; Jude Hemanth et al., 2018; Khamrui et al., 2017), particle swarm optimization (Al-Ta'i et al., 2017), artificial bee colony (Siar et al., 2018). However, researchers have no consensus about the superiority of one of them over the others. Furthermore, each one of them has its strength and weakness. Table 2.8 summarises the characteristics of each of them.

Table 2.8

Characteristics of Optimization Algorithms

Algorithms	Objective	Parameters	Approach	Features	Applications
GA	Genetic algorithms are widely used to produce high-quality solutions to optimization and search problems by relying on bio-inspired operators like crossover, Mutation, and selection	- Population size. - Crossover. - Mutation.	Global search heuristic approach	- High accuracy and convergence depend on Mutation	- Hardware evolution, Robotics, Design automation, and Investment decisions
PSO	Particle swarm optimization (PSO) is a computational approach that optimizes a problem by iteratively attempting to improve a candidate solution on a given quality criterion.	- Position. - Velocity.	The Population-based on stochastic optimization	- Fast to Convergence to the objective but inaccuracy in the result.	- In Computer Sciences, such as face localization, image segmentation, edg detection, image filterings, image denoising, and Industrial Engineering like grid computing and Robotics. (Erdogmus, 2018).
ACO	The ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be overcome to get a good track through graphs	- Pheromone evaporation. - Pheromone weighting	The meta-heuristic algorithm only Two-dimension approach	The convergence speed with the goal does not consider the accuracy of the result.	- Routing in telecommunication networks, Traveling Salesman, Graph Color ing, Scheduling, and Constraint Satisfaction.

Algorithms	Objective	Parameters	Approach	Features	Applications
ABC	The Artificial Bee Colony Algorithm (ABC) is an optimization algorithm focused on the honey bee swarm's intelligent foraging behavior.	- The employed and unemployed foraging bees and food sources	Meta-heuristic algorithm	The convergence performance of ABC is slow.	- In optimizing numerical problems, General assignment problems, Cluster analysis, Constrained problems, optimization, Structural optimization, advisory system, and medical image classification (Kaswan et al., 2015).
HS	Harmony Search (HS) is a population-based metaheuristics algorithm inspired by the musical process of finding perfect harmony.	- Distance bandwidth - Memory size - Pitch adjustment rate - Rate of choosing from memory	Meta-heuristic search	Harmony search is easy to implement, quickly converges to the optimal solution, and finds a good enough solution in a sensible amount of computational time.	- Applied in various engineering fields such as design optimization of heat exchangers, telecommunication, construction, and engineering structures problems (Manjarres et al., 2013).
TS	Tabu Search (TS) is a meta-heuristic algorithm that solves complex combinatorial optimization issues.	Neighbourhood N(s), Tabu list, and Aspiration criteria	Global search Meta-heuristic algorithm		

Given the importance and accuracy of medical information, we need a good algorithm to find the optimal site for the inclusion process into the medical image preserved from distortion, negatively affecting the diagnostic process and, thus, the patient's life. A GA may be considered the best optimization algorithm because it gives accurate results.

A GA is a search algorithm and heuristic technique that mimics the process of natural selection and belongs to a larger class of evolutionary algorithms (EA) (Albadr et al., 2020; Phonsa & Bansal, 2018). GAs commonly generate high-quality optimization for search problems by relying on bio-inspired operators such as Mutation, crossover, and selection (Essa et al., 2018; Kalaiselvi & Kumar, 2016). John Holland introduced genetic algorithms in 1960 as a heuristic optimization approach inspired by the concept of Darwin's theory of evolution, which explains the fitness of an individual in the environment through the approach of natural selection (Abdulateef et al., 2017; Tang et al., 1996). Natural selection is based on the survival of the fittest; weak individuals of each species will die and cannot produce more offspring. The environment chooses the strongest individual to survive and produce more individuals in the next generation. Coding the problem into a genetic representation requires defining the solution as a chromosome representing a potential solution and defining the objective function (fitness function) as a mathematical relationship to assess the quality of each possible solution. The solution with high fitness value will survive and form a new population of the solutions for the next generation.

A chromosome in genetic algorithms, sometimes called a genotype, is an arranged list of genes corresponding to an input domain x that determines the proposed solution to the problem (Ha et al., 2021). According to the solution length (chromosome), there are two

types of GAs. The first is the traditional GA, where the chromosome length is fixed. The second one is the variable-length GA, in which the chromosome length is variable (Handayanto et al., 2018). Currently, fixed-length solution representations dominate for solving problems whose number of variables are known a prior (Stringer, 2007). Still, not all issues are so simple or well understood, and often the size of an acceptable solution cannot be determined in advance (Aliefa & Suyanto, 2020).

In contrast, several variable-length GAs have been proposed to solve design problems to obtain high-fitness solutions with fewer iterations than the traditional fixed-length GA. Several variants of VLC-GAs have been presented in the literature for various applications. For instance, Jiang et al. (2011) suggested a VLC representing QoS-aware multi-path web-service design plans to determine the optimal path using a GA. Also, Brie & Morignot (2005) presented a VLC-GA for a system that solves planning problems, i.e., determining the optimal sequence of actions to reach given objectives. In (2019), Cruz-Piris et al. developed a VLC-GA to solve a multi-path problem in road traffic coordination by dividing the chromosome into cells that encode path branches. In another study (2014), Deif and Gadallah suggested a solution to a wireless sensor network deployment problem by VLC-GA to maximize the coverage range and minimize the deployment cost.

Unfortunately, and to our knowledge, the variable-length genetic algorithm has not been implemented in steganography schemes. Generally, a standard GA comprises six steps: (a) initialization, (b) Fitness function, (c) Selection, (d) Crossover, (e) Mutation, (f) Termination. Below is the description of the standard GA steps.

Step 1: Initial Population refers to randomly generating the first population solutions in the solution space. A chromosome represents the numerical value of the candidate

solution. A chromosome comprises genes representing particular traits (Zainuddin & Abd Samad, 2021).

Step 2: Describe the fitness function f(x) to assess the quality of each chromosome in the research population. High-quality individuals (i.e., chromosomes) comprise the next generation's population (Kadhim & Mosa, 2021; Zainuddin & Abd Samad, 2020). The evaluation process is repeated several times until the termination condition is met.

Step 3: Selection refers to the elite selection process, selecting two chromosomes to produce new offspring. The process of selecting parents is subject to evaluation using the fitness function (Zainuddin & Abd Samad, 2020; Höschel & Lakshminarayanan, 2019). Several distinct selection methods exist in genetics: tournament selection, roulette wheel, ranking, and relative selection.

Step 4: Crossover refers to producing new individuals from the G1 and G2 selected parents (Taher & Kadhim, 2019). Usually, the parents are chosen according to their high fitness value among other chromosomes to ensure that the new offspring acquires strong genes that may produce better generations. The process of creating new offspring is by merging some of the genetic characteristics of the first parent, G1, with another part of the characteristics of the second parent, G2. The new offspring is characterized by the non-repetition of the parents (Albadr et al., 2020; Mohamed et al., 2017). The crossover step is significant in enabling GA to explore the search space more efficiently, thus accelerating the convergence velocity (Koohestani, 2020). There are several methods of intersection operators, such as one-point, two points, and k-point crossover (Zainuddin & Abd Samad, 2021).

Step 5: Mutation refers to producing new individuals by altering some of the genes of the offspring's chromosomes within a certain probability. The mutation operator aims to

prevent genes from getting stuck in local optimum bounds by conducting exploratory searches in the environment to maintain population diversity. Usually, these operations lead to discovering a globally optimal or near-optimal solution to a given problem (Koohestani, 2020).

Step 6: Termination, a new offspring is created and passed on to subsequent populations after selection, crossover, and Mutation are completed. These processes are repeated until the stopping condition is met (Taher & Kadhim, 2019). The stopping condition is an expression or a mathematical equation that has two cases (i) if the number of iterations exceeds the specified generations number or (ii) when the fitness value for the best solution does not change (i.e., if there is a convergence in the results). Figure 2.8 shows the typical process of the GA.

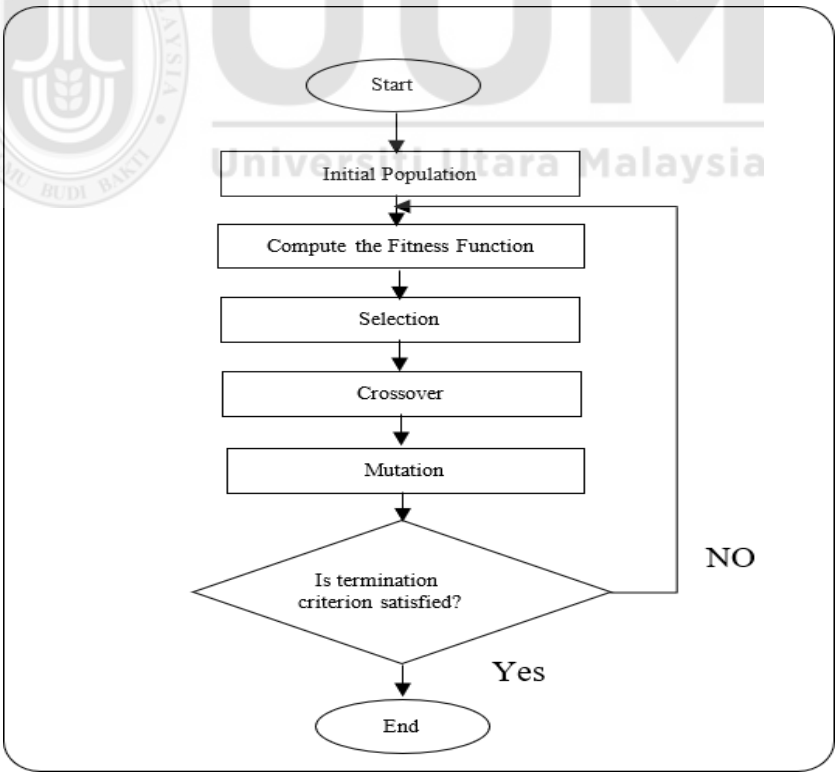


Figure 2.8 The Genetic Algorithm Framework (Höschel & Lakshminarayanan, 2019)

2.8 Evaluation Criteria for Steganography

Generally, steganography algorithms must fulfill some fundamental requirements that conflict. Various characteristics should be investigated to evaluate the strength and drawbacks of the steganography methods. The essential requirements are as follows (Rajesh & Singh, 2015).

(i) Imperceptibility: This criterion is the first and most important requirement because steganography's strength lies in its power to be unobserved by the human eye (Hashim et al., 2018). In other words, the stego and original cover object should be perceptually identical (Abdulwahed, 2019).

(ii) Capacity (payload): Embedding capacity is an important criterion when designing a steganographic system. The capacity denotes the number of bits safely embedded into a particular media file without causing statistically significant modifications (Usha et al., 2014).

(iii) Robustness (Resistance): Robustness refers to the capability of the stego-medium to resist various types of manipulations. In other words, the embedded secret data is challenging for attackers to remove or modify illegally (Dalal & Juneja, 2019; Singla & Juneja, 2014; Raftari & Moghadam, 2012).

(iv) Security is a crucial criterion of any steganography system, referring to the inability of the audience to see the hidden information (Koppu & Viswanatham, 2018; Kumar & Singh, 2015).

(v) Reliability: Reliability is also one of the essential criteria that features a steganography system utility based on the hidden secret data being retrieved error-free. In other words, a successful steganography system must allow users to obtain

confidential information without a loss (Wazirali, 2016; Almohammad & Ghinea, 2010).

It is worth noting that achieving the maximum embedding payload and the highest degree of robustness simultaneously with an agreeable level of undetectability is undoable. Improving one requirement might negatively influence others (Kuo et al., 2015; Jain et al., 2012). Therefore, it is necessary to compromise between robustness, undetectability, and embedding of payload. The excellent balance between these three constraints differs for various applications, depending on the application's requirements (Li, 2005). For instance, increasing the embedding capacity causes noticeable artifacts, which reduce stego-file quality and become accessible to detectability and vice versa (Fadhil, 2016; Al-Mohammad, 2010).

Each steganography method has strengths and weaknesses points. Evaluating steganography systems is essential for a concrete decision when selecting a suitable technique or system. No standard measure or test assesses the technique or system's effectiveness or performance. Nonetheless, general guidelines should be considered when developing a steganography method, as mentioned by (Cox et al., 2008). The fundamental parameters that should be measured to assess the steganographic system's performance are similar between cover and stego-mediums, length of the secret data, and the detection of the secret data's existence or contents (Lin, 2011).

2.8.1 Evaluation of Imperceptibility Criteria

There are various methods and techniques for evaluating imperceptibility in steganography schemes (Akhtar, 2016). These differences are primarily based on the

cover file type applied to conceal information. Ensuring no visual variation between the cover carrier and the stego carrier is essential. For example, the image quality can represent the undetectability of image-based steganography. At the same time, the existence of data hidden in a specific text file can be determined based on the file size. These could also be considered criteria for detecting secret information or data.

The imperceptibility of this difference should be perfect as far as HVS is concerned. If the stego quality is high, then the steganographic system's imperceptibility is also high. Hence, the quality of the stego carrier should be evaluated because it is a vital criterion in assessing the performance of the steganography techniques (Wazirali et al., 2014).

Image quality criteria aim to determine and assess quality through various indicators (Juneja, 2014). Quality criteria are conducted to understand similarities between a raw input image and a processed image, precisely their spatial and spectral properties. When applied in steganography, the raw image is referred to as the cover image, while the processed image refers to the stego-image. Categorizing the image quality criteria is broad since it is based on objective criteria to provide computational criteria in assessing the sameness between the stego image and cover (Ramu & Swaminathan, 2016). Similarly, criteria for subjective quality are used as a basis for the quality image score through an inspection of the images using the HVS.

All criteria for the quality of images help determine the variation between the picture cover and the stego image (Hashim et al., 2018; Ganesan & Bhavani, 2013). Table 2.9 indicates the performance criteria utilized to measure the steganographic image quality.

Table 2.9

The Quality Criteria in an Image Steganography

Quality criteria	**Purpose/Outcome**	**Formulas**
Mean Square Error (MSE)	-To measure the difference between (the original and stego images) - Low MSE means high quality	$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[C(i,j) - S(i,j)]^2$
Peak to Signal Noise ratio (PSNR)	-To measure the similarity between (the original and stego images) - High means high quality	$PSNR = 10\log_{10}[\frac{M\ x\ N}{MSE}]$
Normalized cross-correlation (NCC)	- To measure the similarity between the cover image and the stego-image. - Whenever the NCC value is close to 1, the stego-image is similar to the cover image.	$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)\ x\ S(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}$
Average Different (AD)	- AD provides the average of change concerning the cover and stego image. - Ideally, it should be zero.	$AD = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(C_{ij} - S_{ij})}{MN}$
Root Mean Square Error (RMSE)	To measure distortion, which should not be noticeable.	$RMSE = \sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(C_{ij} - S_{ij})^2}$
Structural Content (SC)	- To measure the difference between (the original and stego images). - The high value of SC shows that the image is of low quality.	$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C_{ij}^{\ 2}}{\sum_{i=1}^{M}\sum_{j=1}^{N} S_{ij}^{\ 2}}$

Quality criteria	Purpose/Outcome	Formulas
Maximum difference (MD)	- To measure the difference between (the original and stego images). -The large value of MD means that the image is of poor quality.	$MD = \max\left(\left\|C_{ij} - S_{ij}\right\|\right)$
Normalized Absolute Error (NAE)	- To measure the difference between (the original and stego images). - The high NAE value shows that the image is of poor quality.	$NAE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(\lvert C_{ij} - S_{ij}\rvert)}{\sum_{i=1}^{M}\sum_{j=1}^{N} C_{ij}}$
Structural Similarity Index Metric (SSIM)	- To evaluate the similarity between the cover image and the stego-image. - The SSIM value is limited in the range (0,1) if the SSIM value is close to 1, indicating that the stego-image is the same as the cover image and has high quality.	$SSIM(C,S) = \frac{(2\mu_C\mu_S + c_1)(2\sigma_{CS} + c_2)}{(\mu_C^2\mu_S^2 + c_1)(\sigma_C^2 + \sigma_S^2 + c_2)}$

2.8.2 Evaluation of Capacity Criteria

Steganography mainly provides secret communications by embedding confidential data within a cover carrier. Therefore, calculating the length of the data concealed in the cover is necessary. According to Cox et al. (2008), steganography and embedding capacities are not equivalent. The embedding capacity is the maximum number of bits inserted into the cover carrier. The message should be embedded to preserve the image quality without changing size (Iyer & Laktharia, 2016).

In contrast, the steganography capacity indicates the payload size that can be securely inserted into a cover carrier using a particular embedding process, i.e., the maximum number of undetectable bits in the cover carrier where the probability of detection is negligible (Filler et al., 2009). Generally, the steganography capacity is less than the embedding capacity. It is difficult to determine the maximum number of undetectable embedded bits. Table 2.10 indicates the performance criteria utilized to measure the steganographic image capacity.

Table 2.10

The Capacity Criteria in An Image Steganography

Capacity criteria	Purpose/Outcome	Formulas
bits per pixel (bpp)	- The maximum of data can be concealed and restored positively.	$bpp = \frac{Number\ of\ secret\ bits\ embedded}{Total\ pixels\ in\ the\ cover\ image\ (H\ x\ W)}$

2.8.3 Evaluation of Security Criteria

The undetectability is the main aim of any steganography technique (i.e., no one can identify between the original and the stego images). Steganography security is classified into 1) statistical steganalysis and 2) embedding efficiency. The best scenario is that the detection likelihood is no more than a random guess (Fridrich & Lisonek, 2007). It could also be practically tested to estimate the probability of detection by looking at the specific current

steganalysis methods. Steganography is complemented by steganalysis. Steganalysis' primary purpose is to detect the existence of concealed messages. Most steganalysis algorithms look for artifacts caused by the message-concealing process (Mewalal & Leung, 2018).

Nonetheless, a completely secure steganographic approach is almost impossible since they insert the confidential data into the cover medium's fundamental component and thus change it. Alternatively, steganographers determine the security of the embedding process by its relative likelihood of detection. Several factors influence the detectability of data concealed in a stego-carrier (Li et al., 2011; Fridrich et al., 2006), such as:

i) The cover carrier selection.
ii) The selection rule identifies cover elements that might be modified during embedding.
iii) The embedding operation that modifies the cover elements, and
iv) The number of embedding changes (directly related to the secret data length)

2.8.4 Evaluation of Robustness Criteria

Robustness refers to the difficulty needed to destroy embedded data, i.e., embedded confidential messages cannot be removed after a credible detection by target attacks, depending on the full knowledge of the embedded algorithm, excluding knowing the secret key (Ghebleh & Kanso, 2014). Many attacks may detect or change secret information like rotation, scaling, cropping, compression, and filtering.

The steganography algorithms should resist such as these changes. Table 2.11 indicates the performance criteria utilized to measure the steganographic image robustness.

Table 2.11

The Robustness Criteria in An Image Steganography

Robustness criteria	Purpose/Outcome	Formulas
Chi-square (X^2)	- Robustness tests technological steganography's ability to survive attempts to remove confidential information after the attacks were applied to stego-image. - If the variation is slight (i.e., near zero), that means no information inside the image; if the difference is close to one, the image held data.	$X^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$
Normalized Cross-Correlation (NCC)	- If the NCC values are equal to 1, it implies that the stego-image resulting from the algorithm is entirely resistant to image processing attacks.	$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)\ x\ S(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}$

2.9 Medical Image Dataset

In image steganography schemes, a collection of images constitutes the dataset. This dataset is used to validate the rightfulness of the developed image steganography schemes and benchmark the findings by comparing them to existing state-of-the-art literature. This research utilizes the grayscale standard Images' three types of datasets: chest, retina, and brain, as reliable datasets, where each image pixel consists of 8 bits for these datasets. Ten images from each dataset were used for evaluation, in size 512 x 512 and grey color. These original images were downloaded from the following websites: (i) the Chest dataset obtained from the URL https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia, (ii) the Retina dataset obtained from the URLhttps://www5.cs.fau.de/research/data/fundus-images, and (iii) the Brain dataset obtained from the URLhttps://www.kaggle.com/datasets/jakeshbohaju/brain-tumor.

2.10 Related Work

Cryptography and information hiding are essential tools to secure data security during transit. Information hiding has flourished in the last few years because it hides the presence of messages on the cover; unlike cryptography, it does not provoke attacks. Much research is currently underway to solve security issues by the steganography system based on spatial domain, especially in the LSB technique. Due to the limitations of the LSB technique, many researchers have worked to improve it and release updated versions of LSB, including ISB and DISB (Mohammed, 2015; Zeki & Manaf, 2009). However, ISB and DISB techniques have been applied only with watermarks (Mohammed et al., 2014). In addition, both were cited for having constraints regarding capacity, quality, and robustness (Parah et al., 2012).

A method to protect sensitive medical image data was proposed by Mantos and Maglogiannis (2016); the secret sharing steganographic approach protects the ROI portion of a medical image (DICOM). Patient data and hash values of the sensitive data were embedded into the Region of Non-Interest part of a medical image; hash value helps the integrity of an ROI of a medical image. The main drawback of this approach is the extraction method of ROI and embedding method. Another major limitation is more space consumption while embedding the ROI data into the RONI of a medical image. Another proposed method to secure medical image information is based on encryption and steganography techniques by Al-Dmour and Al-Ani (2016). In this work, the coding technique encoded the patient information and embedded it into the pixels of the region of non-interest (RONI) of the patient's medical image without affecting the pixels of the region of interest (ROI). Critical shortcomings of the system are: 1) it does not focus on the ROI portion, which has been affected by a disease and is considered an essential part of the diagnostic process. ii) There are fewer protection criteria to preserve the patient's visualized reports, such as MRI scans. iii) protect only the patient secret information.

Also, introduced an approach known as an adaptive threshold detector (ATD) by Yang et al. (2017) to enhance image quality, which automatically divides the area into a region of interest (ROI) and a non-region of interest (NROI) into two different parts. This method improves image quality and has a high data embedding capacity. Additionally, it approximates ROI and NROI before adding the data to them. This method avoids overflow and underflow information while side information, like segmentation information, is embedded as additional information. Additionally, semi-reversible data-steganography technology was proposed by Loan et al. (2017) for medical images and general examinations. Using the substitution of LSB and ISBs, the patient's electronic patient data/record (EPR) was merged. Rivest Cipher4 (RC4) encryption algorithm has also been used to give a double layer of security to EPR/embedded data. The proposed scheme can handle high payload and is semi-reversible and computationally efficient. At the same time, Sun (2016) suggested an edge-based secret image embedding method that uses a canny edge detector with 2k correction (where 2k correction maintains the visual quality). Firstly, a Canny edge detector is applied to detect the edge of the cover image, and only edge pixels are selected for embedding the payload. Secondly, the sorting method randomizes edge pixels to enhance security. Moreover, Huffman coding has also been applied to achieve compression and protect private data, but it is detected by modern steganography analysis, i.e., lack of robustness.

Parah et al. (2015) proposed a high-capacity data-hiding technique using edge detection techniques and even-odd pixel separation. Changes in edge pixels are less noticeable to the human eye than changes in non-edge pixels because edge pixels correspond to high frequencies of the image. For hybrid edge detection, use Canny and Prewitt techniques to separate even and odd sub-planes of the green and blue planes, while the red plane stores the edge/non-edge pixel state. The experimental results were compared to contemporary data-hiding techniques. The comparison results demonstrated that the proposed approach has a high degree of

imperceptibility and embedding capacity; more edge pixels are extracted than the conventional method, but computational complexity is increased. Many previous research works used the GA to integrate the information into the cover or carrier image to improve image quality and robustness (Mohamed et al., 2011; Zamani et al., 2009).

Moreover, several steganography systems have applied the GA technique to select the embedding location before embedding the secret data to improve security (Nosrati & Karimi, 2012). Although it prevents the detection of embedded secret data by altering the statistical characteristics of the blocks of pixels, it requires extra processing time for secret data of a sizeable amount while minimizing stego-image distortion. Therefore, it is crucial to embed the secret data in a reduced time efficiently. Shah and Bichkar (2021) employed the LSB substitution steganography technique. The secret message bits are randomly embedded into the LSB of each pixel in the fixed-size blocks that make up the cover image. For a particular block of the cover image, use the genetic algorithm to identify the starting point of the embedding, the direction in which the confidential data should be entered, and the polarity of the confidential data. Polarity seeks to determine if confidential data must be updated or kept unchanged. A new method for concealing sensitive information in the spatial domain was put forth by Mohsin et al. (2019) and is based on the particle swarm optimization (PSO) algorithm. The host and secret images are split into four sections. PSO is used to determine the best starting point for message embedding and the direction of sensitive information in a grayscale image to maximize embedding capacity and maintain the quality of the stego-image.

Another method proposed by Kanaan and Nazeri (2014) relies on the genetic algorithm-based method for visual image quality tuning and lossless data in the spatial domain (GA). The fundamental concept of the proposed technique is to formulate the image steganography problem as a search and optimization problem to find the optimal scanning direction and starting point for the host image. The starting point is another option that can be considered

when developing the concept for the proposed technique. In other words, the researchers (Kanan and Nazeri) selected a starting point with a different raster order than the base point (first column and first row) of the host image point pair; the proposed method produced better results than the classical start point. The data were included based on the simple LSB technique to ensure acceptable quality of the stego-image after finding the best starting point.

2.11 Summary

Recent years have seen the emergence of steganography as an essential system in the research and evolution of data security on the World Wide Web (WWW). Furthermore, the rapid growth of information technology and the related attacks by intruders have compelled scientists and engineers of the computer to develop more intelligent algorithms for hiding sensitive and personal information freely transmitted via the internet. Various embedding techniques have been proposed to handle the steganography issues. In this regard, a comprehensive review of the most recent literary works is presented, which provides knowledge on the state-of-the-art understanding of this area of research. Based on the information presented about LSB in this chapter. It can be said that the technique can be modified and improved to become a suitable technique for image steganography, especially in telemedicine. The next chapter will elaborate on the research methodology planned for this research to be carried out.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

As presented in the previous chapter, this research aims to address the problem of image steganography as a combinatorial optimization problem by avoiding the implicit constraint that leads to local minima traps. More specifically, this research aims to provide better imperceptibility and security of the secret message embedding inside the host image by enabling more scattering in the embedding. Unlike previous approaches, which assume that the secret message should be inserted into a connected area within the host image, the development in this thesis should make no such assumption. Adding more degrees of freedom to optimization typically results in more decision variables and vast solution space. Consequently, this raises concerns about the optimization algorithm's convergence. Therefore, to ensure convergence, this research proposes a novel concept named n-Decomposition Genetic Algorithm-based steganography (n-DGA), which will call a chain of genetic connectivity instead of a single genetic depending on the user input variable named n. The role of the n value is to balance efficiency and effectiveness, which is regarded as an application-dependent variable.

This chapter will detail the methodology carried out in this research, arranged as follows: Section 3.2 presents the research methodology. Section 3.3 describes the implementation hardware and software design. Then, the datasets are introduced in section 3.4, followed by the summary in section 3.5.

3.2 Research Methodology

This research will be carried out in five phases to assist in managing the objectives effectively, as depicted in Table 3.1. The table shows that the first phase starts with the initial investigation by conducting the theoretical literature survey to derive the research gap from the relevant works conducted in the field of information concealment. Next, the second phase includes formulating the problem and reducing the solution space. It proceeds with the third phase, developing the proposed technique (n-DGA) by defining the control parameter for computational cost flexibility. The fourth phase integrates the schemes' design, including the embedding and extraction processes. Finally, the fifth phase will be implemented to evaluate the performance of the proposed scheme based on several determining criteria and compare it with the benchmark using several datasets.

Table 3.1

Research Methodology

Phases	**Activities**	**Outputs**
Phase 1	**Initial Investigation** - Understand of Digital Steganography Domain - Getting Problem Statement - Investigation of the State-of-Art for the Image Steganography	- Problem Statement - Research Questions - Research Objectives - Scope
Phase 2	**Formulation of an Embedding Scheme** - Problem Formulation - Reduction of Solutions Space and Constraints	- Objective (1)
Phase 3	**Decomposition Schemes** - Secret Message - Controlling Parameter	- Objective (2)
Phase 4	**Integrate the Schemes into the Proposed Technique**	- Objective (3)
Phase 5	**Evaluation of the Proposed Technique** - MSE, PSNR, and Correlation - RS Analysis, Histogram Attack	- Objective (4)

3.2.1 Phase 1: Initial Investigation

This phase aims to critically analyze the existing research to identify the issues that need further research and investigation to support the existing research. This analysis is based on various sources, including previous research published in reputable journals, conference articles, and books. Securing information about patients by embedding them in their medical images is a trade-off between security and imperceptibility (Ramu & Swaminathan, 2016). The former refers to the immunity to various attacks to determine the information. The latter refers to maintaining the visual quality of image information to ensure an accurate diagnosis based on the image from the medical expert. The security implies changing specific values of pixel intensities to avoid statistically-based attacks or brute force attacks, which implies specific degradation of the visual image quality. On the other side, preserving the image's original information implies the occurrence of some hidden statistical patterns that lead to concealing the secret message by a successful attack. Maintaining both goals simultaneously is an open research problem (Kadhim et al., 2019; Muhammad et al., 2017).

Reading the literature, various embedding approaches can be derived, mainly from the spatial and frequency domains (Gajabe & Ali, 2022; Wazirali et al., 2019; Shah & Bichkar, 2018). In each of the two categories, various models and techniques are used. This research is interested in LSB, which aims to insert the secret bits inside the selected positions of the least significant bits inside the pixel. This technique is favored because of its simplicity, capacity, and light computational weights as it deals with the image in its original space without needing frequency transformation (Shah & Bichkar, 2020). However, it is vulnerable to statistical attacks (Reshma & Vinod Kumar, 2020). This research aims to develop a steganography approach that solves this matter by meeting various performance metrics. It incorporates the power of random searching integrated with heuristic knowledge under the framework of evolutionary genetic algorithms.

3.2.2 Phase 2: Formulation of an Embedding Scheme

An encoding of the problem is needed to solve it using the evolutionary genetic optimization framework. Encoding means the conversion from the application space to the geneo-space. The role of this conversion is to enable conducting the subsequent genetic steps to solve the problem. As mentioned, the first objective is to formulate an implicit scheme to avoid invalid implicit constraints by defining the decision variables and their constraints and thus defining the solution space.

The decision variables (mostly, but not always, represented as a vector x) represent aspects of the problem over which the decision-maker controls (Boyles, 2015). The embedding information (decision variables) consists of seven information types that must be presented to the algorithm, as shown in Table 3.2. First, define the direction, which indicates the pixel scanning direction of the host image, using 16 directions, as is shown in Table 3.3. Second, the X-offset which the offset of the starting point of embedding in the x-direction. The third is the Y-offset, which defines the y-offset of the starting point of embedding in the y-direction. Fourth, bit-planes define using the least significant bit to insert the secret message. Any subset of the four least significant bits might provide 16 possible states, as in Table 3.4. Fifth, SB-pole indicates to secrete bit-pole value. It takes one or zero, so inverting the bit is enabled when the value is 1. Sixth, the secret bit direction (SB-Dir) has two possible directions. Lastly, bit plane direction (BP-Dir) also has two directions. Table 3.5 shows the values of the last three genes: SB-pole, SB-Dir, and BP-Dir.

Table 3. 2

The Representation of Kanan & Nazeri (2014) That is Used for Encoding the Bits Insertion Within One Block

Gene-Name	Value-Range	Length (No. of Bits)	Characterization
Direction	0-15	4 Bits	The Host Image Pixels Scanning Direction
X-offset	0-15	4 Bits	X-offset of Starting Point
Y-offset	0-15	4 Bits	Y-offset of Starting Point
Bit-Planes	0-15	4 Bits	Using LSBs to Insert Hidden Bits
SB-Pole	0-1	1 Bit	The secret Bit Pole value
SB-Dir	0-1	1 Bit	The direction of Secret Bits
BP-Dir	0-1	1 Bit	The direction of Bit Planes

The first gene in the proposed chromosome is the direction, which means the pixel scanning direction. Table 3.3 displays potential values for the direction. There are 16 potential orders for pixel scanning direction.

Table 3.3

Possible Values for Direction Gene

Direction	**Rows**	**Columns**	**Type**	**Arrangement**
0	Up to down	Left to right	Triangle	Columns then row
1	Up to down	Right to left	Triangle	Columns then row
2	Down to up	Left to right	Triangle	Columns then row
3	Down to up	Right to left	Triangle	Columns then row
4	Up to down	Left to right	Square	Columns then row
5	Up to down	Right to left	Square	Columns then row
6	Down to up	Left to right	Square	Columns then row
7	Down to up	Right to left	Square	Columns then row
8	Up to down	Left to right	Triangle	Rows then columns
9	Up to down	Right to left	Triangle	Rows then columns
10	Down to up	Left to right	Triangle	Rows then columns
11	Down to up	Right to left	Triangle	Rows then columns
12	Up to down	Left to right	Square	Rows then columns
13	Up to down	Right to left	Square	Rows then columns
14	Down to up	Left to right	Square	Rows then columns
15	Down to up	Right to left	Square	Rows then columns

Bit-Planes are used in host pixels to determine LSB planes to insert hidden data. Table 3.4 displays potential values for the Bit-Planes.

Table 3.4

Possible Values for Bit-Planes Gene

Value	Characterization	Value	Characterization
0000	Use None of the LSBs	1000	Use 4th LSB
0001	Use 1st LSB	1001	Use 1st and 4th LSBs
0010	Use 2nd LSB	1010	Use 2nd and 4th LSBs
0011	Use 1st and 2nd LSBs	1011	Use 1st, 2nd, and 4th LSBs
0100	Use 3rd LSB	1100	Use 3rd and 4th LSBs
0101	Use 1st and 3rd LSBs	1101	Use 1st, 3rd, and 4th LSBs
0110	Use 2nd and 3rd LSBs	1110	Use 2nd, 3rd, and 4th LSBs
0111	Use 1st, 2^{nd,} and 3rd LSBs	1111	Use 4 LSBs

Table 3.5 includes additional information about the last three genes (SB-Pole, SB-Dire, and BP-Dire), indicating possible values for each.

Table 3.5

Possible Values for SB-Pole, SB-Dire, and BP-Dire Genes

Gene Name	Value	Characterization
SB-Pole	0	In this state, no modifications are made to secret bits
	1	In this state, all secret bits are modified to be suitable
SB-Dire	0	In this state, no modifications are made to secret bits
	1	In this state, secret bits are reversed from end to beginning
BP-Dire	0	In this state, bit-planes are utilized from MSB to LSB
	1	In this state, bit-planes are utilized from LSB to MSB

Mathematically, the solution space defines as a set of elements. Each element has the length of the size of the secret message multiplied by the total number of pixels in the host image to encode the pixel's position for insertion and by a whole number ranging from 1 to 4 to encode the considered bits for insertion.

$$x \in X \subset \mathbb{N}^{S \times 2}$$

$$\|Solution\ Space\| = (4k)^S$$

$$k = m \times n$$

However, considering that two bits in the secret message cannot be inserted in the exact bit location in the image, then the size of the solution space is reduced as follows:

$$\|Reduced\ Solution\ Space\| = (4k)(4k-1)(4k-2)\ldots(4k-S+1)$$

Based on the above, the problem is a combinatorial optimization problem with a large solution space. For a more efficient search, several constraints are incorporated. For example, pre-defined insertion directions and pre-defined blocks for embedding, i.e., blocks number with their locations.

3.2.3 Phase 3: Decomposition Algorithm

The second objective is to propose a secret message decomposition scheme to cater to the lack of convergence in the searching procedure and the flexibility of application customizability. This section provides the developed embedding methodology named n-Decomposition Genetic Algorithm-based Steganography (n-DGA), shown in Figure 3.1. The optimization algorithm is designated as n-Decomposition Genetic-based steganography (n-DGA). The concept extends the benchmark (Kanan & Nazeri, 2014), which assumes a fixed length of solution space by restricting the insertion of the connected region. In contrast, in the n-DGA, the secret message can be inserted over the image with various disconnected areas based on the number n that the user sets.

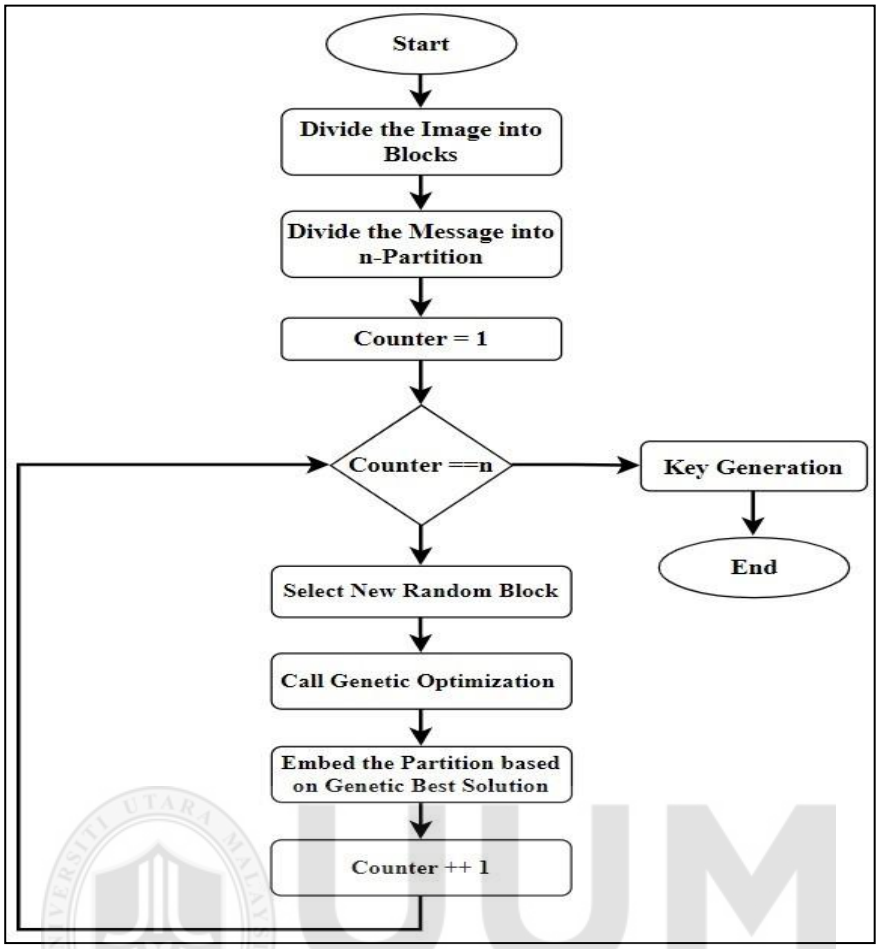


Figure 3.1 Embedding Methodology of n-DGA

The principle of n-DGA working based on Figure 3.1, the algorithm will perform some operations:

(i) Decompose the original $I_h(m,\ n)$ image into $I_h(m_b,\ n_b)$ image. Depending on the QL value, which is input, the number of horizontal and vertical blocks is calculated as follows:

$$m_b = \lceil \frac{m}{QL} \rceil \quad (3.1)$$

$$n_b = \lceil \frac{n}{QL} \rceil \quad (3.2)$$

Where:

QL denotes the quantization level

m_b number of blocks in the height of the image

n_b number of blocks in the width of the image

Points out that each value of m, n, m_b, n_b, and QL affects the length used for encoding the X and Y offset for chromosomes, as given in example (1).

Example (1)

Assuming an image combined of 600*400 pixels, QL=50, and the secret message size is 200 bits. Assuming the following solution.

$m_b = 12$; $\frac{600}{50} = 12$ (i.e., needs 4-bits to represent 12)

$n_b = 8$; $\frac{400}{50} = 8$ (i.e., needs 3-bits to represent 8)

(ii) The secret message is divided into parts based on the value of n, a parameter that controls the number of times the genetic algorithm is called.

(iii) The exact representation of Kanan & Nazeri (2014) is used for inserting the secret message in any block that will be used. The representation is given in Table 3.2.

The n-DGA used many parameters. They are given in Table 3.6 with their meaning.

Table 3.6

Parameters of n-DGA- Parameters of n-DGA

Symbol	Meaning
m_b	Number of blocks in the height of the image
n_b	Number of blocks in the width of the image
QL	Denotes the quantization level
n_j	The number of jumps for inserting the secret message
$n_{used-blcoks}$	The number of used blocks
$Max - iteration$	The maximum number of iterations for the searching
$Safe\ distance$	The minimum distance needed for validating the new jump for insertion

This research proposed a new variant, n-Decomposition Genetic Algorithm Based-Steganography (n-DGA). This new variant ensures the variable-length searching attribute by generating sub-spaces for optimization, each with one length. The traditional fixed-length genetic optimization algorithm is called for each subspace, as shown in Figure 3.2. After the

n-DGA algorithm decomposes the secret message into n equal parts, it searches for the best location to embed those parts into the host image. Hence, the image pixels that included the secret message part have become a forbidden area to hide the remaining parts in subsequent iterations. Moreover, the overall solution consists of the individual solutions obtained by all the total iterations.

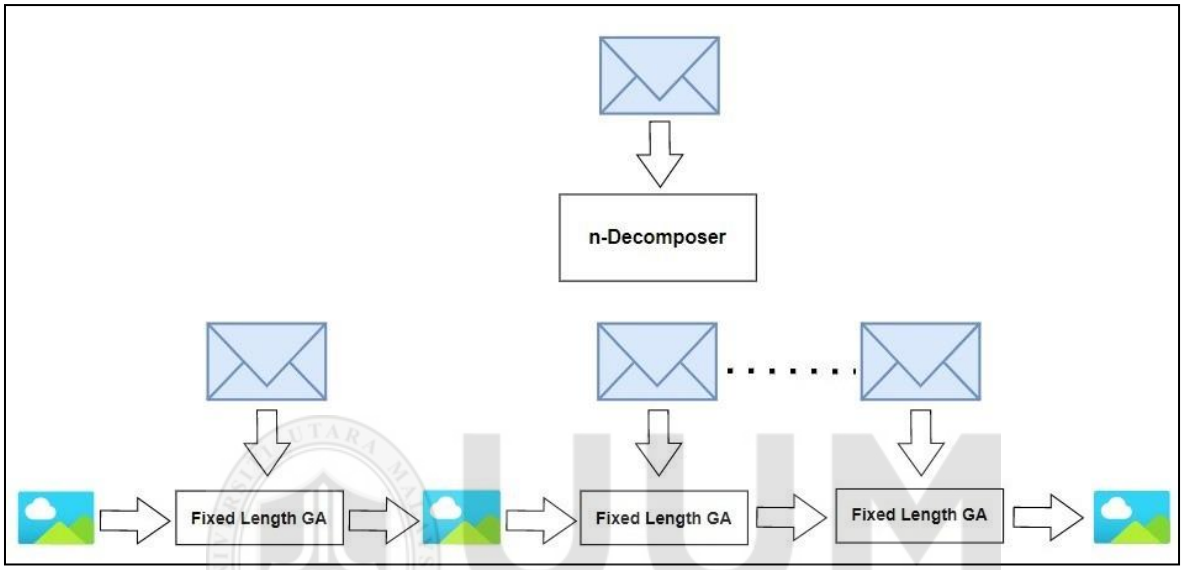


Figure 3.2 Block Diagram for Showing the Functionality of the n-Decomposer Algorithm for Variable-Length Embedding

Figure 3.3 depicts the design of n-DGA. As demonstrated, the design of n-DGA begins with providing multiple inputs to the algorithm. The inputs consist of the maximum number of iterations, the number of divisions, a safe distance indicating the minimum distance between two blocks, the number of blocks in height, and the number of blocks in width. The algorithm then begins the iteration counter and division counter. Next, the algorithm iterates through the iterations and the divisions one by one, performing GA with the fitness function on each division. The algorithms accept the secret message and the stego-image while performing the embedding and calculation of the fitness function.

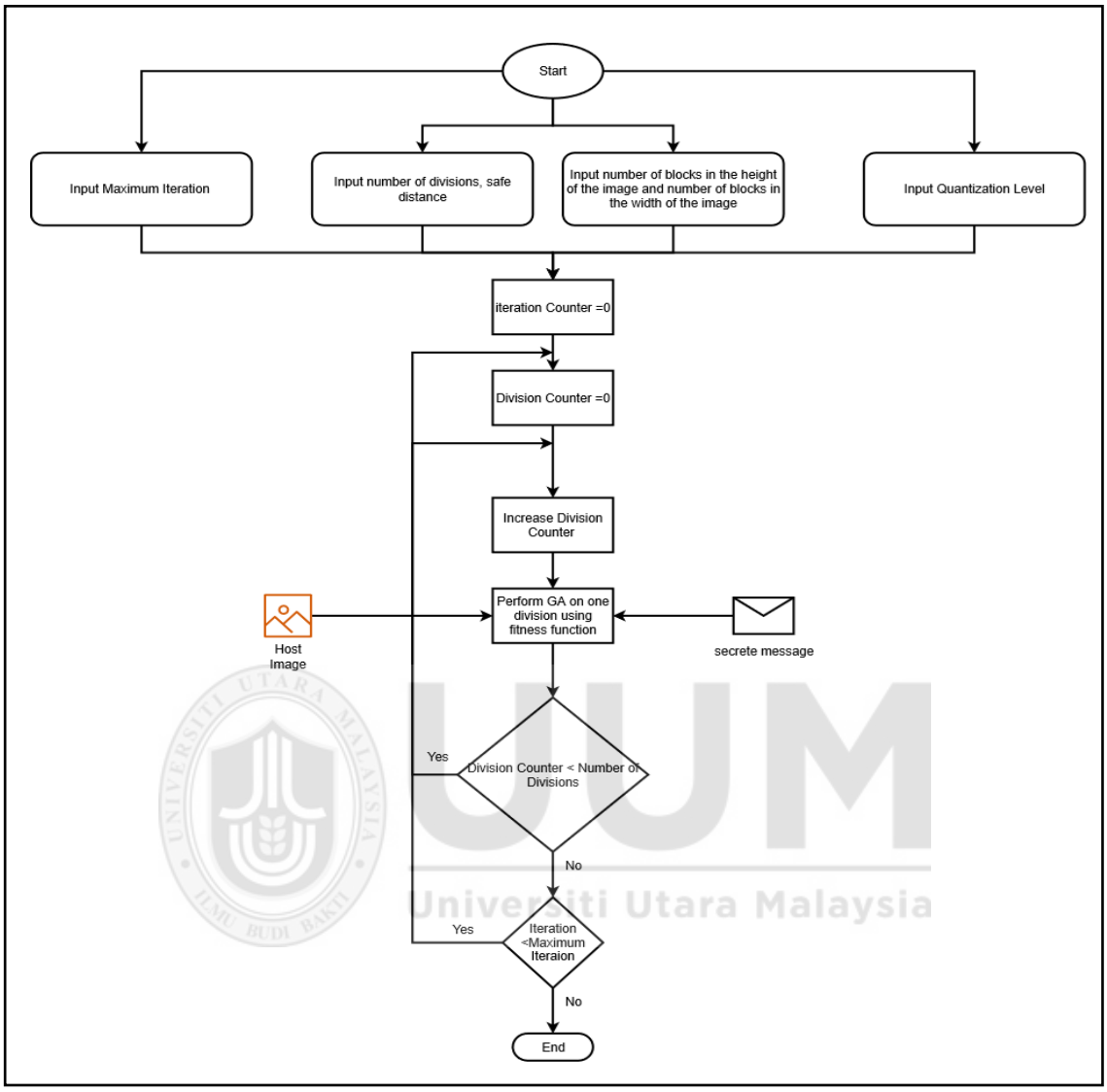


Figure 3.3 Design of n-DGA

3.2.4 Phase 4: Integrate the Proposed Schemes into a Technique

This research aims to improve the imperceptibility and security of the medical image steganography scheme using n-Decomposition Genetic Algorithm Based-Steganography (n-DGA). It was designed to hide secret data in the medical image, using the least significant bit (LSB) technique to achieve imperceptibility and security. The n-DGA proposed technique includes the Formulation of an Embedding Scheme and the Decomposition Algorithm scheme for providing computational cost flexibility. The steganography scheme consists of multiple

sub-stages: a (i) preparation of the data, including the secret message and the host image. (ii) the process of embedding the secret message within the host image, and (iii) the process of extracting the secret message.

(i) Data Initialization: It is a data preparation stage, such as converting a secret message into binary bits. The data entered includes: the secret message to be hidden in the host image is a series of letters and symbols. The secret message is subjected to pre-processing by converting it into ASCII codes and then binary bits to match the representation of the host image pixels. Furthermore, dividing it into n-parts according to the value of n for achieving the objectives of the proposed n-DGA method, as shown in Figure 3.4.

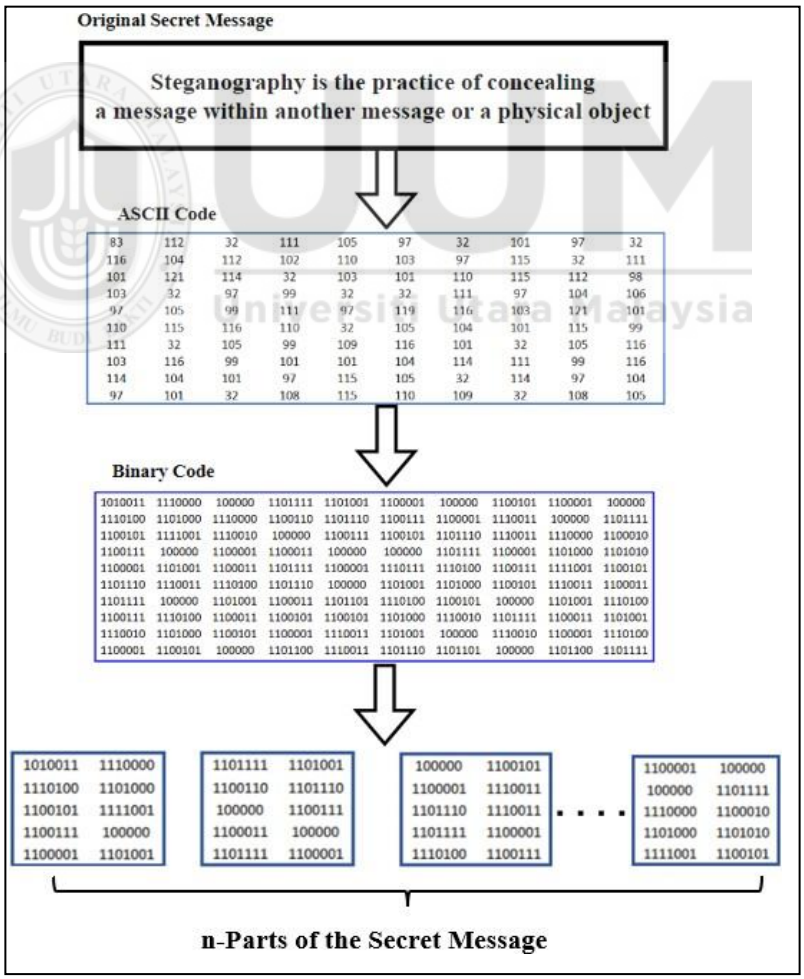


Figure 3.4 Secret Message Preparation

Also, before the embedding process is performed, the original image selected from the dataset is used in steganography as a host image to hide the secret message.

(ii) Embedding Process Stage: This research proposed a new n-Decomposition Genetic Algorithm Based-Steganography (n-DGA) scheme to conceal a secret message in medical images using the steganography technique. The embedding process goes through a set of logically sequential stages. It begins by defining the space for genetic research that depends on decision variables and the constraints set on some of those variables. Then is followed by the design of the n-DGA algorithm to embed data inside the host image to maintain imperceptibility and security as much as possible. The proposed system is based on inserting a secret message's text inside a host image, which will protect the secret until it reaches the recipient, who can decipher the secret message utilizing the same stego-key proposed by the sender. Therefore, the attacker cannot discover the secret, and even if he does, they will be unable to find it. The proposed embedding process includes two stages, n-DGA and LSB, which work together to produce a secure stego-key. The first stage (n-DGA) is responsible for dividing the secret message into parts depending on the value n parameter. Then, it searches for the best location to embed the secret message. After determining their location in the first stage, the second stage is responsible for embedding the secret message bits into the host image.

Figure 3.5 depicts a flowchart for evaluating fitness function based on chromosomes generated from a genetic algorithm (GA). The proposed algorithm requires initializing the host's image and the secret message to generate a population of chromosome-dependent initial solutions for the search process. After that, performing crossover and mutation operations to generate other solutions that may be more efficient than the parents. These solutions are evaluated and repeated until a final solution is reached for each portion of the message.

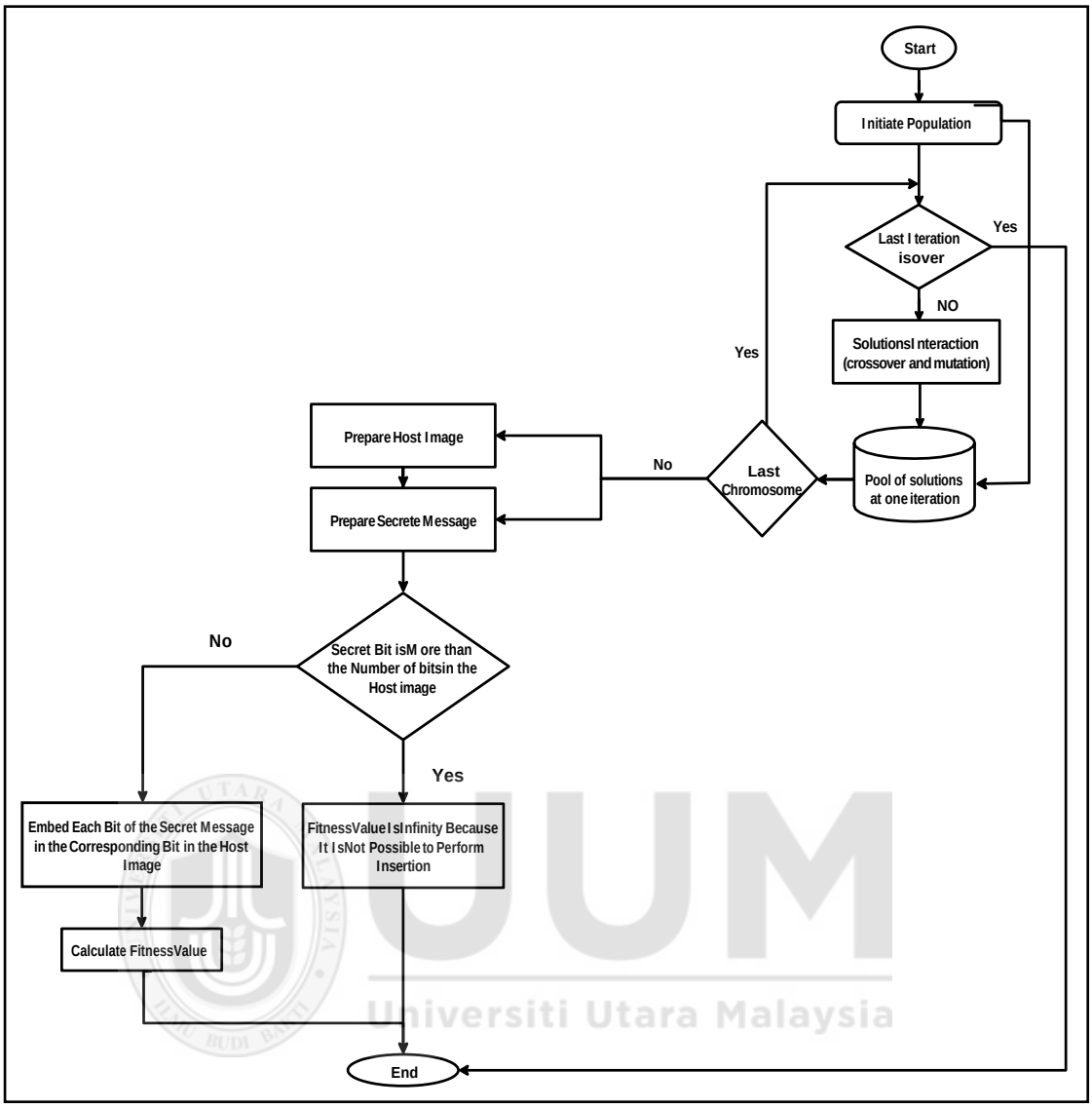


Figure 3.5 Methodology of Evaluation of Fitness Function

(iii) Extracting process Stage: A standard steganography system includes two primary phases: embedding and extraction. The embedding algorithm enters the secret bits into a carrier medium: text, audio, image, or video. In contrast, the main objective of the extraction algorithm is to retrieve the secret bits of the embedded secret message from the host. The procedures of the extraction algorithm are easier than the embedding algorithm because it follows the same embedding procedures but inversely and according to the agreement between the sender and receiver in advance.

Steganography integration can be maintained by guaranteeing that concealed information can be obtained correctly and is easily readable without any concern of their alteration. Utilizing the stego-key, which is demanded to initiate the process of embedding or extraction, is one way to increase steganography security. A stego-key renders the extracting process computationally impossible for unauthorized users (Nabi & Afzal, 2020; Almazaydeh & Sheshadri, 2018). Hence, without the stego-key, it is nearly impossible to complete the extraction procedure. The proposed image steganography scheme performs the extraction algorithm on the receiving side.

The decomposition of the stego-image's pixel is carried out according to the algorithm previously agreed upon by the sender and receiver. The embedding algorithm embeds the secret bits into the host image on the sender side. It then produces essential helpful information for extracting the hidden information from the receiving side. This information is stored in the stego-key immediately, and the stego-key updates until the embed process is finished. Additional information that saves the stego-key includes the number of parts of the secret message, the direction of scanning the image, the starting point, and the number of bits used. Usually, the extraction algorithm has two procedures; the first is a general procedure for all steganography systems and is the opposite of the procedures of the embedding process. The second procedure is extracting information from the stego key to extract the secret message bits and grouping all 7 bits to form a single character, thus obtaining the complete secret message. Figure 3.6 depicts the steps for extracting the message fragments one by one until the entire secret message embedded within the host image has been recovered.

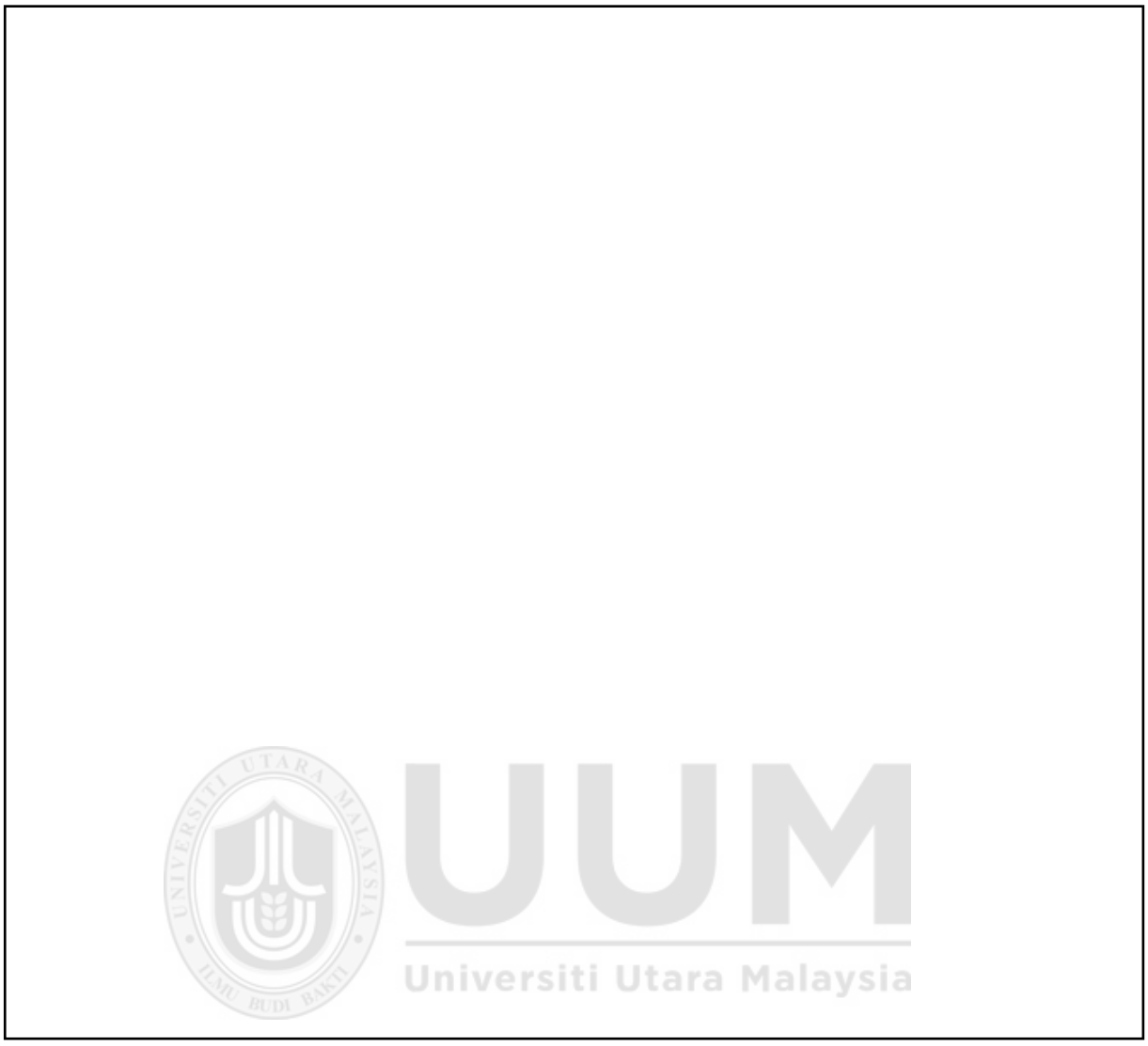


Figure 3.6 Extraction Process

3.2.5 Phase 5: Evaluation

The last objective is evaluation; the algorithm is compared to Kanan and Nazeri (2014) benchmark. The comparison is based on two main criteria: imperceptibility and security. Security is an indicator of a system's resistance to steganography attacks. Steganography is considered successful if the attacker cannot detect the hidden information. Security can be achieved in two ways. (1) The inability of the human eye to distinguish between cover images and stego images (the quality of the resulting image) or the use of statistical analysis to reveal hidden information. (2) If traces of hidden information are detected, the attacker cannot

retrieve that information. The measures for the criterion of imperceptibility are correlation, mean squared error (MSE), and peak-signal-to-noise ratio (PSNR). The evaluation criteria for the security criterion are histogram and RS.

(i) Imperceptibility and Distortion measure: embedding the secret message into the host image produces a stego-image. The stego-image should be unnoticeable, which means the distortion should be imperceptible. The imperceptibility (i.e., quality) of the stego-image is measured by comparing it with the host image using (1) MSE, (2) PSNR, (3) correlation, and other criteria (Seyyedi & Ivanov, 2014).

(1) The MSE criterion measures the statistical difference in pixel values between the host and the stego-image.

(2) The PSNR measures the similarity between the stego-image and the host, i.e., how these images are close.

MSE and PSNR criteria are very rapid and easy; therefore, they are widely utilized. MSE and PSNR are defined below:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{w} \sum_{j=1}^{H} (A_{mn} - B_{m})^2 \quad (3.3)$$

$$PSNR = 10 \log_{10} [\frac{W \; x \; H}{MSE}] \quad (3.4)$$

Where:

A_{mn}, B_{mn} Are the host image, the stego-image, and W, H are the dimensions of the images, respectively. The μ_A and μ_B denote A and B mean values, respectively.

The low value of MSE means a high value for PSNR due to the inverse relationship between the MSE and PSNR. A higher value to PSNR means slight deformity. It is

excellent if the PSNR value exceeds 40 decibels (dB). It could be passable if it is between 30 dB and 40 dB, but if the value of PSNR is less than 30 dB, it is inadmissible because the deformity is very high (Ranjith Kumar et al., 2016).

(3) Correlation (r) is a performance metric that measures the similarity between the host image and the stego-image. Whenever the r value is close to 1, the stego-image is similar to the host image. r is defined as below:

$$r = \frac{\sum_m \sum_n (A_{mn} - \mu_A)(B_{mn} - \mu_B)}{\sqrt{(\sum_m \sum_n (A_{mn} - \mu_A)^2)(\sum_m \sum_n (B_{mm} - \mu_B)^2)}} \quad (3.5)$$

(ii) The security measure, the main requirement of any steganography technique, is the inability to detect. So, the steganography technique must be robust and reliable to resist steganography analysis attacks. Evaluating security can be tested using a variety of steganography analysis schemes. This work used RS analysis and histogram.

(1) The pixel difference histogram (PDH), a type of statistical attack used to detect hidden secret data (Rahman et al., 2020; Arumugham et al., 2018), is frequently regarded as the most effective method for evaluating the robustness of a stego-image by observing the characteristic artifacts left by the embedding of LSB to pixel values in the histogram (Kini, N. G. & Kini, V. G., 2019).

(2) RS analysis is one of the most efficient methods for analyzing the LSB steganography technique, which is used to validate the LSB's security. RS is accomplished by analyzing the dual statistics of the host and stego-images to determine whether a host image contains a secret message (i.e., identifying the host file's flaw) and the length of that secret message (Mewalal & Leung, 2018; Manoharan, 2008).

3.3 Implementation Design

To implement the proposed technique to improve the embedding competence of digital medical image steganography. The following hardware and software capabilities are described in Table 3.7.

Table 3.7

The Requirements for Hardware and Software

Hardware / Software requirement	Feature
Processor	Intel (R) Core i5-8250U @ CPU 1.6GHz 1.8 GHz
Display	16 HD widescreen 1920 X 1080
Memory (RAM)	4.00 GB (3.88 GB usable)
System Type	64-bit Operating System
Hard Drive size	1000 GB
Windows edition	Windows 10
Programming language	MATLAB simulation

3.4 Datasets

A dataset in a steganography system is a collection of images used to compare this investigation's findings to previous literature. Many images are used as a dataset in the literature, and each researcher derives certain conclusions from them. The current thesis uses the same procedure to evaluate and benchmark the experimental findings that realistically utilize the proposed method—the image datasets used in the proposed technique for practical purposes described in this subsection. Three image datasets were used with grayscale, namely: (a) chest dataset using the URL (https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia), (b) retina dataset the URL https://www5.cs.fau.de/research/data/fundus-images, and (c) brain dataset using the URL https://www.kaggle.com/datasets/jakeshbohaju/brain-tumor. Kaggle, a well-known online community platform for scientific research, was utilized to acquire dataset images due to the images' availability and no cost. Images extracted from datasets are reliable for various fields,

including the medical field. Table 3.8 describes the number of images for each (Chest and Brain) obtained from the Kaggle platform and Friedrich-Alexander-Universität.

Table 3.8

The Details of Dataset Images

Platform	Dataset	No. of Images
Kaggle	Chest	234
Kaggle	Brain	36
FAU	Retina	18

Figure 3.7 shows the datasets used in the proposed framework; each dataset consists of ten images of (a) the Chest, (b) the Retina, and (c) the Brain.

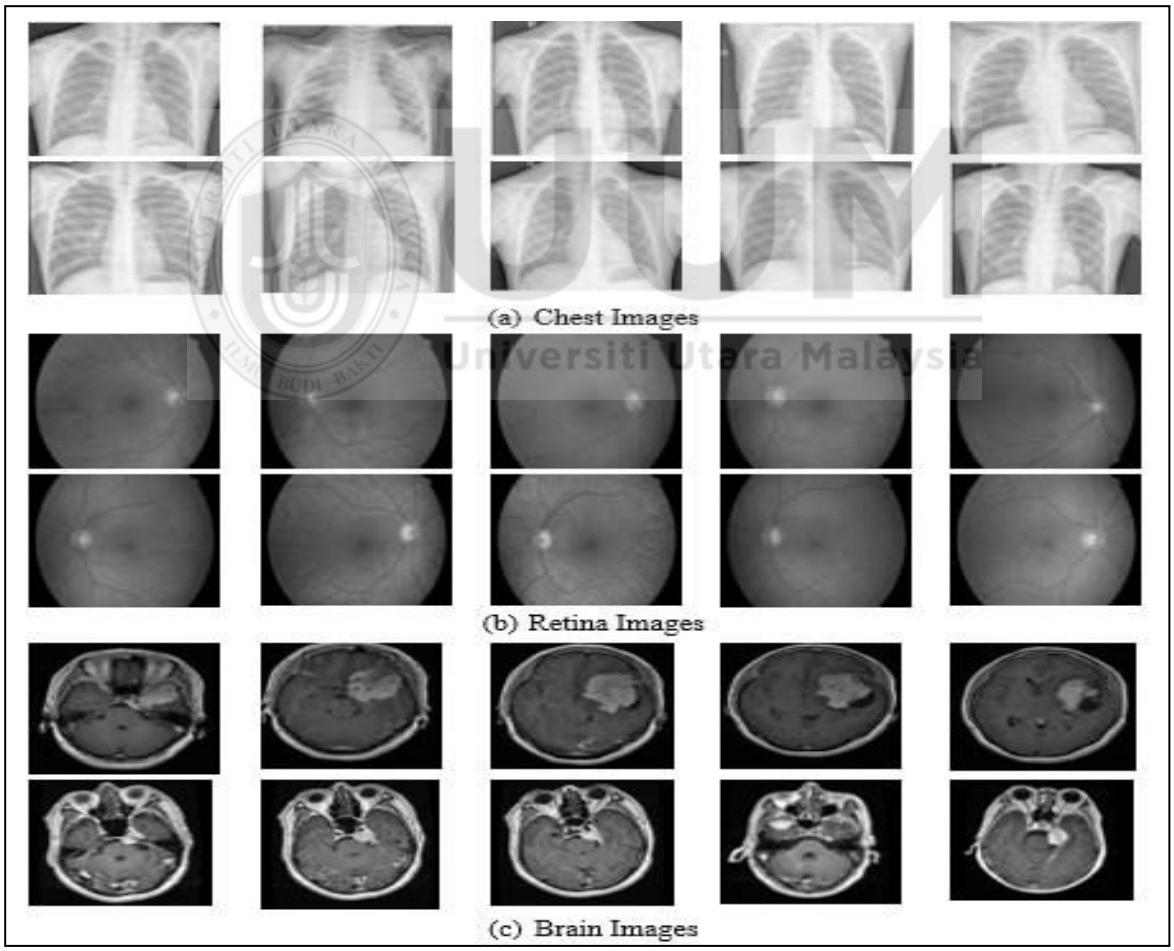


Figure 3.7 The Datasets Used in the Proposed Framework, (a) Chest, (b) Retina, and (c) Brain Images

3.5 Summary

This chapter provided a novel steganography development for enabling efficiency and effectiveness trade-offs based on user-provided parameter n. The chapter introduced the methodology of the n-Decomposition Genetic Algorithm-based steganography, formulation of embedding, decomposition algorithm for computational cost flexibility, integration of design n-DGA schemes, implementation design, and datasets. The difference between the developed algorithm named n-DGA and the literature algorithms is that the former enables more scattering of the secret message embedding in the host image without changing the solution space size. Consequently, this makes it similar in convergence performance and better in imperceptibility and security. The next chapter will explain the n-DGA proposed technique.

CHAPTER FOUR
PROPOSED TECHNIQUE: n-DECOMPOSITION GENETIC ALGORITHM-BASED STEGANOGRAPHY SCHEME

4.1 Introduction

The chapter details the proposed technique known as n-DGA, where the chapter is divided into several sections. Section 4.2 introduced the proposed technique. Next, in section 4.3, image and message preparation is presented, followed by section 4.4, the embedding process. Section 4.5 presents the extracting process. Afterward, section 4.6 explains the validation of the proposed technique. Finally, the discussion and summary are in Sections 4.7 and 4.8, respectively.

4.2 The Proposed Technique

Typical steganography consists of four primary processes: (1) data preparation, (2) embedding, **(1)** extraction, and (4) validation. The proposed technique is known as the n-decomposition genetic algorithm based on a variable-length search comprised of two schemes, namely; (1) Decision Variables and Solution Space Scheme and (2) n-DGA scheme. These schemes are involved in the embedding process, as illustrated in Figure 4.1.

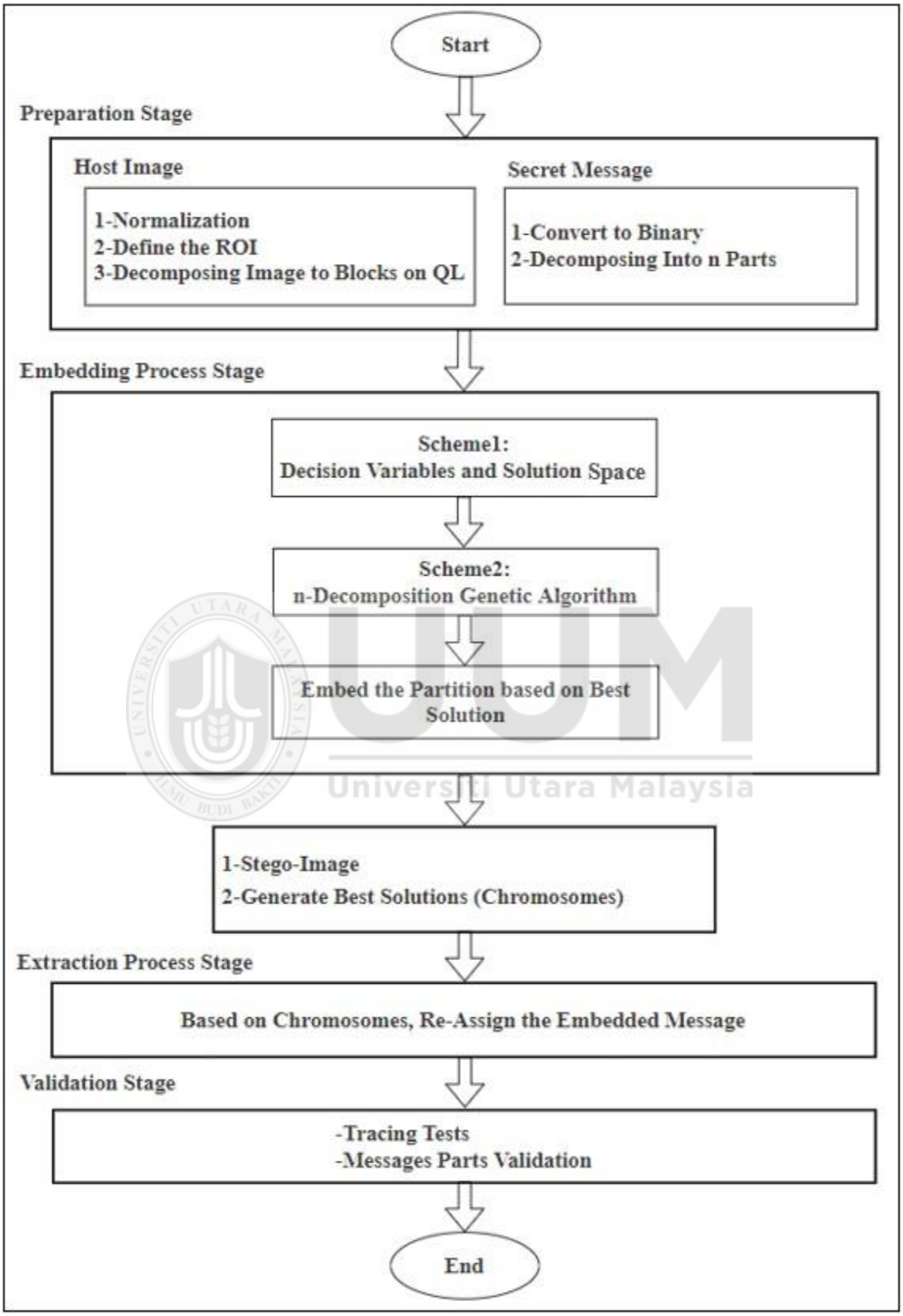


Figure 4.1 The Framework of the Proposed Technique

The following section will elaborate on each process involved, starting from the data preparation to the extraction process, by emphasizing that the proposed technique was involved in the embedding process.

4.3 Preparation Stage

This section presents the first stage of the n-DGA-developed steganography scheme. It starts with message and image preparation. Generally, before embedding in a steganography scheme scenario, the sender must select a suitable carrier for inserting the message (e.g., image, text, audio, or video). Regarding the inputs, the preparation stage requires selecting an image from a pre-defined dataset and considering it a cover image to conceal the secret message. Preparing both image and secret message co-occur as it is regarded as the beginning of the work of the steganographic scheme that precedes the embedding process (Akhtar, 2016; Fadhil, 2016).

The message decomposition has been stated as an objective in chapter one. Its goal is to attain more degree of freedom for embedding. The message hidden in the host image is a string of characters. Each character in the secret message is subjected to processing to transform into ASCII code, then a series of binary bits before embedding it to match the host image. Converting the secret message to bits is essential for any digital steganography scheme. The message is prepared by decomposing it into n parts according to the number of sections provided by the user or selected by the application. As a reminder, the n control parameter provides customizability flexibility higher to the user. Efficiency is obtained with a lower value of n, while higher effectiveness is obtained with a large number of n.

The size of the message affects the solution space significantly. The relation between the message size and the solution space is given as

$$SS = 4nm \times (4(nm-1)+3) \times (4(nm-1)+2) \times (4(nm-1)+1) \times 4(nm-1) \ldots \times 4(nm-(S+1)) \quad (4.1)$$

Where:

SS denotes the size of the solution space

S denotes the size of the message

It shows that the insertion of bits of messages is significantly high and affected by the size of the message. Hence, the convergence of the optimization will be affected too. To mitigate this effect, the message is partitioned into smaller parts leading to a significant reduction in the solution space.

The original image selected from the dataset is used in steganography as a cover to hide the secret message before the embedding process is performed. The image is prepared based on defining its dimensions, which can be represented in two dimensions, size (mxn). Each image comprises finite elements, each having a specific location and intensity. The elements are known as image pixels, $P = \{p_1, \ldots, p_n\}$, where each greyscale pixel consists of 8 bits: $[p_i] = 8$, $p_i = \{b_1, \ldots, b_8\}$, where b_j is in the set range {1,0}. Sometimes the cover image is addressed during preprocessing steps such as (1) normalization to be suitable for embedding, noise reduction, or segmentation. This work resizes the host image to 512 * 512 pixels. Next, (2) define the restricted area, i.e., region of interest (ROI), which cannot be used for embedding by the steganography algorithm. This area can be set by an expert using a mask. (3) The original image $I_h(m, n)$ is decomposed into several horizontal and vertical blocks, depending on the quantization level's (QL) value. Assuming all images are embeddable, images were selected from three datasets: chest, retina, and brain, chosen because they are considered the most common examples of image-based medical diagnoses.

4.4 Embedding Process Stage

The integration process begins once the formulation of the embedding scheme and design of the decomposition algorithm scheme. The embedding proposed technique goes through a set

of logically sequential stages and is responsible for inserting the message into the medical image. In scheme 1: Decision variables and solution space, the problem is encoded into geneo-space that depends on decision variables and constraints set on some variables to avoid invalid implicit constraints such as insertion directions and embed blocks. Meanwhile, in scheme 2: n-DGA, the algorithm divides the geneo-space into n sub-spaces and then calls the GA n-times, equal to the number of subspaces, to search for the optimal decision variables. The LSB technique is then used to embed the secret message based on the optimal solutions for each part. This section includes three sub-sections: Sub-section 4.4.1 introduces scheme 1: Decision Variables and Solution Space. Next, scheme 2: n-DGA is presented in subsection 4.4.2. Next, the embedding based on the n-DGA is presented in sub-section 4.4.3.

4.4.1 Scheme 1: Decision Variables and Solution Space

Optimization refers to finding a set of inputs for an objective function whose outcomes maximize or minimize a given quantity (Dhiman & Kaur, 2018; De León-Aldaco et al., 2015; Gendreau & Potvin, 2014). Inputs (independent parameters) may be subject to some limitations to improve the objective function. Parameters that can be altered in searching for the optimal solution are named decision or control variables. The restrictions imposed on the permissible parameter values are referred to as constraints. Decision or control variables are believed to affect the output significantly. Selecting the optimal set of decision variables can be challenging because it is hard to determine which variables influence each specific simulation behavior. The logic that determines control flow is also a decision variable. Typically, the domain of potential values for decision variables is limited by user-specified constraints. The optimization problem consists of three elements: (1) the decision variables, (2) the constraints, and (3) the objective function. Formulating an optimization problem entails translating a "real-world" problem into the equations and variables mathematically that represent these three elements.

The inputs of the problem are a host image I_h, which has the size of $m \times n$ and a message M with the size of S. The goal is to select a subset of pixels from I_h for inserting the bits of M by allowing only the usage of the four least significant bits (FLSB) for embedding, considering that the selected subset of pixels is a vector x. Then the optimization problem is formulated as given in Equation 4.2.

$$x = argmin\ (f(\ I_h, I_s(I_h, M, x))) \qquad (4.2)$$

Where:

I_h Denotes the host image

I_s Denotes the stego image, which is the image after embedding the message M based on the solution x inside I_h

f Denotes the fitness value of the solution x when it is used for inserting M inside I_h.

The embedding configuration includes the different decision variables the optimization algorithm provides for specific embedding solutions. In the benchmark approach, much information was used for embedding: direction, offset, Bit-Planes, secrete pole value, and direction of both secrete and bit planes. The meaning of this information is presented in the previous chapter in Table 3.2. in the sub-section 3.2.2. They will be used in adaptive embedding for the proposed algorithm with some changes.

The first change is the offset value measured in the benchmark approach by the number of blocks into which the host image is divided. However, the offset of the proposed algorithm will be measured by the pixel, which means that no quantization is performed. The second change is to define a subset of pixels to embed message bits, i.e., allow only the four least significant bits (FLSB) for embedding. Another modification is the direction. The benchmark approach included a diagonal direction in the embedding, while the proposed algorithm excluded the diagonal direction. The reason is to prevent affecting the information in the main part of the image where the diagonal information exists. These changes made are constraints on the

decision variables. Hence, the new embedding information of the proposed algorithm is depicted in Table 4.1.

Table 4. 1

The Embedding Information as Part of the Chromosome in the Proposed Algorithm

Gene-Name	Range	Length (No. of Bits)	Characterization
n	0-10	4 bits	It determines the number of portions in which the message has been divided
Direction	0-15	4 Bits	The Host Image Pixels Scanning Direction (diagonal direction is excluded)
X-offset	0-W	Variable	X-offset of Starting Point as pixel index
Y-offset	0-H	Variable	Y-offset of Starting Point as pixel index
Bit-Planes	0-15	4 Bits	Using LSBs to Insert Hidden Bits
SB-Pole	0-1	1 Bit	The secret Bit Pole value
SB-Dir	0-1	1 Bit	The direction of Secret Bits
BP-Dir	0-1	1 Bit	The direction of Bit Planes

The proposed chromosome includes eight genes, which are listed in Table 4.1. The first gene is the controlling parameter n for the number of message portions. This gene is responsible for dividing the message into divisions that will be inserted in separate portions in the host image. The second gene is the direction of the pixel scanning direction. The possible values of this gene are depicted in Table 3.3. in the sub-section 3.2.2. Due to the pixel scanning direction having 16 potential orders, it is represented as the four-bits gene. Figure 4.2 presents the values of the first four bits with the corresponding order assuming the image has a dimension of 3x3.

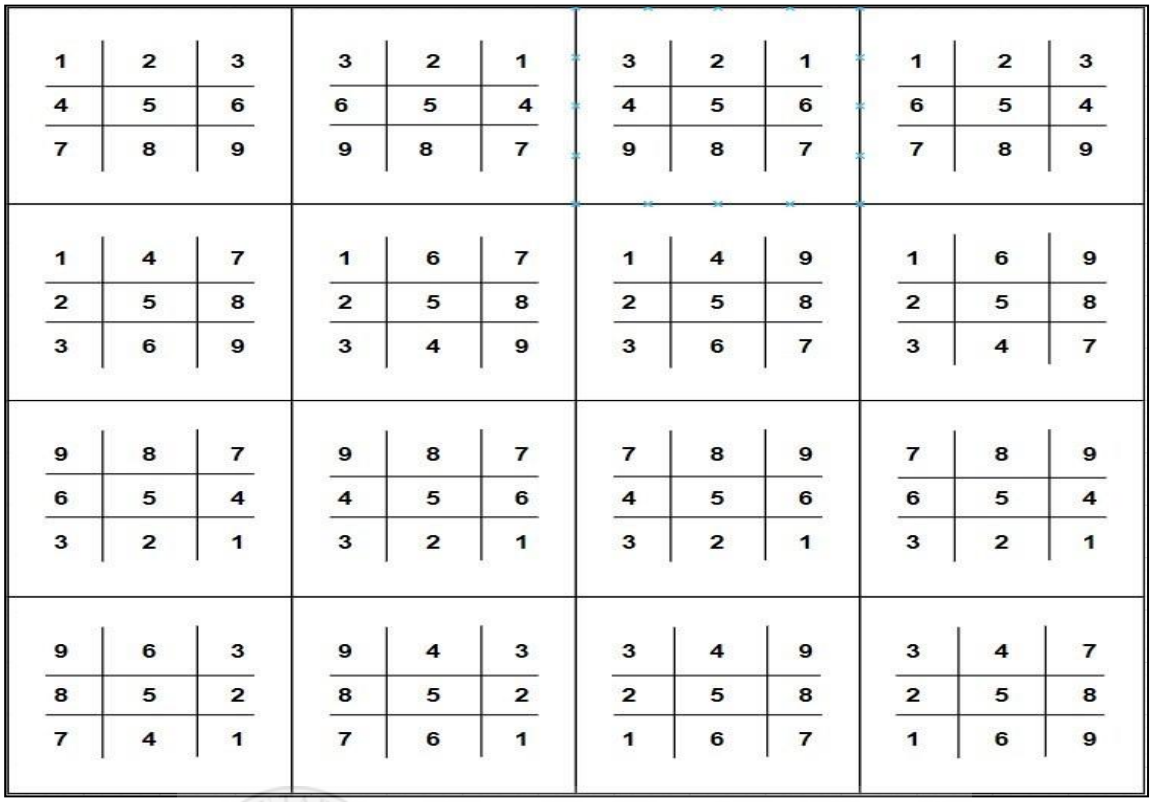


Figure 4.2 The Different 16 Directions Based on the Configuration

For example, in case 0, the first pixel is used for insertion in the top left. Then the next right pixel is taken until the end of the row. Afterward, the second row starts in the same direction as the previous one until the message ends.

Two genes, X-offset and Y-offset, represent the starting point, each having a variable length. The first one is the offset of the starting point of embedding in the X-direction, and the second one defines the Y-offset of the starting point of the Y-direction. X-offset and Y-offset are used as pixel indexes of the starting point, which are mean pixels' positions. The other gene is the Bit-Planes, which determine the LSB planes of the host pixels that embed confidential data into the host image. Table 3.4. in the sub-section 3.2.2 displays the possible Bit-Planes values. The main component of an image is the pixel (the smallest part of the image); any operation performed on the image means dealing with this part. Each pixel has an index of its location and a value representing the intensity of the color. In grayscale images, the color is indicated by a single eight-bit pixel to achieve the color range (0-255) through the pixel value 2^8. The

greyscale resolution indicates the slightest discernible alteration in an image's shades or levels of grey. Black is the darkest color, and white is the lightest shade of grey. In contrast, the color images represent the color by combining the three primary colors: red, green, and blue (RGB). Hence, the color image needed 8 bits for every pixel, i.e., (24 bits) as shown in Figure 4.3.

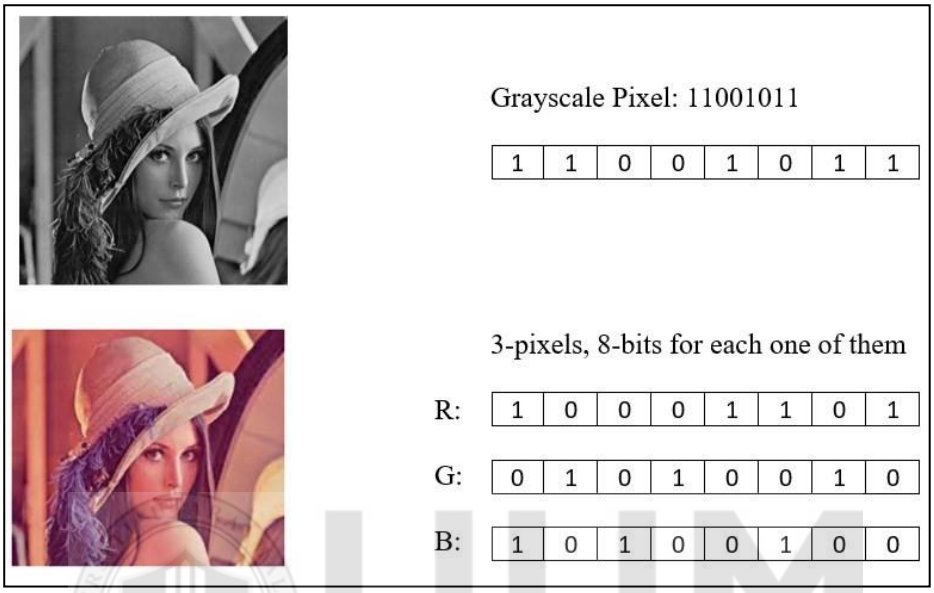


Figure 4.3 Bit-Planes Distribution in Greyscale and Color Images

The last three genes, SB-Pole, SB-Dir, and BP-Dir, specify the secret Bits-Pole value, the secret bits' direction, and the LSB planes' direction, respectively. Table 3.5 in sub-section 3.2.2 indicates possible values for the three genes. The pseudocode of extracting the decision variables from the chromosome is presented in Algorithm 4.1.

It takes the chromosome as input and provides the various decision variables as output. They are given as direction, x-Offset, y-Offset, Bit-Planes, SB-Pole, SB-Dir, and BP-Dir. It is considered that decimal values represent the components inside the chromosome, and each has a particular index. The pseudocode shows that each decision variable is read according to its index. In line 6, the goal is to find the number of used bits in the four LSB for Embedding.

Algorithm 4.1: Extracting the Decision Variables

Input:

Chrom

Output:

direction, X-offset, Y-offset, Bit-Planes, SB-Pole, SB-Dir, BP-Dir

Start:

```
direction=chrom (1); // the value 1 indicates the first component
X-offset =chrom (2);
Y-offset =chrom (3);
Bit-Planes = mappingBitPlanes (chrom (4));
Bit-Planes =dec2bin(Bit-Planes,4);
numOfUsedBits=length(find(Bit-Planes =='1'));
SB-Pole =chrom (5);
SB-Dir =chrom (6);
BP-Dir =chrom (7);
```

end

The solution space's size depends on the number of bits used for embedding. Considering that four bits from each pixel were allocated as candidate bits for embedding and that the total number of pixels in the image is $k = m \times n$ then the total number of possibilities for bits insertion is related $4K$, and it can be calculated as:

$$kP_s = \frac{K!}{(k-S)!\,S!} \qquad (4.3)$$

Where S denotes the message size, LSB-based 8-bit grayscale image steganography schemes directly handle the least significant bits to maintain the resulting image quality (stego-image). Still, they have limitations on the low imperceptibility of stego-images when using more bit-planes to conceal a secret message (Srayyih Almaliki, 2019). Figure 4.4 shows the distortion level on a greyscale image pixel.

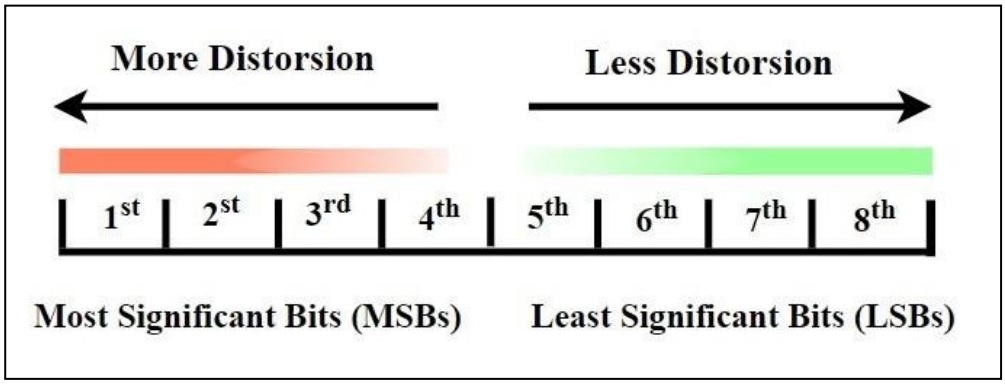


Figure 4.4 The Binary Representation of One Grey Pixel

This work uses the genetic algorithm to solve the problem of data hiding in k-LSBs of the host image when k is large. For example, GA works well if the secret data is embedded in the k-LSBs of the host image, where k is less than or equal to three (3). However, it works poorly if k is greater than three (3) because the possible substitutions will grow exponentially as k increases. For example, assume that k=4, there are (2^4)! =16! Possible substitutions (about 20,000 billion) can be used to embed data (Mohamed et al., 2011; Wang et al., 2001). The goal of specifying a subset of pixels from I_h to insert the bits of M is to allow only the use of the four least significant bits (FLSB) for embedding and considering that the selected subset of pixels is a vector x. Then the optimization problem is formulated as given in Equation 4.1.

The role of the objective function is to evaluate the performance of the candidate solution. In n-DGA, the definition of the objective function is given as an option to the user. One possible definition is to use mean square error (MSE) between the stego-image and the host image. However, it is also possible to use other measures within the objective function, such as SSIM and Correlation. Generally, the below pseudocode algorithm for the general steps of the chromosome evaluation is shown in Algorithm 4.2.

Algorithm 4.2 The Objective Function Calculation

Input

Chromosome

Message

Host image

Output

Fitness value

Start

```
reqBitSeq=ChooseRightSecretSeq(sbPole,sbDir);
messageLength=length(reqBitSeq(:));
chromBitSeq=ConvertChromToBitSeq(chrom);
chromLength=length(chromBitSeq);
[messReq,chromReq,status]=DetermineRequiredNumberOfPixels(messageLength,chromLength,numO
fUsedBits,length(imCover(:)));
if ~status
   fitVal=0;
   return;
end
[messPixelSeq,chromPixelSeq]=CreateHostPixelSeq(oldChromPixels,xOff,yOff,
    direction,messReq,chromReq);
if any(ismember(messPixelSeq,forbiddenAreas))
   MSE = inf;
else
stego=EmbeddingTheMessage(reqBitSeq,chromBitSeq,bitPlanes,bpDir,imCover,messPixelSeq,chrom
PixelSeq);
[~,MSE] = measerr(uint8(imCover),uint8(stego));
end
fitVal=MSE;
```

End

4.4.2 Scheme 2: n-Decomposition Genetic Algorithm

The n-DGA used a variable length search feature by dividing the message into n equal parts. Each part has a corresponding solution space calling the traditional fixed-length genetic optimization algorithm to search for the best location to embed those parts into the host image. Thus, the message parts can be inserted into different unconnected areas based on the number

n defined by the user. Hence, the image pixels that included the message part have become a forbidden area to hide the remaining parts in subsequent iterations. Moreover, the overall solution consists of the individual solutions obtained by all the total iterations. This section presents n-DGA for (i) single decomposition and (ii) multiple decompositions.

(i) Genetic Algorithm for Single Decomposition

Genetic optimization aims to search randomly based on the initialized number of chromosomes denoted as population. After convergence or meeting the stopping criteria, the algorithm selects the best fitting solution as the optimal and uses it for the embedding. This is followed by an iterative process of solutions interaction using two operations, namely: crossover and mutation, for generating better fitting solutions, then selecting the elites for using them again for solutions generations. Four operations must be elaborated to present the entire genetic algorithm: initialization, crossover, mutation, and selection. They are presented with the depicted flowchart in Figure 4.5.

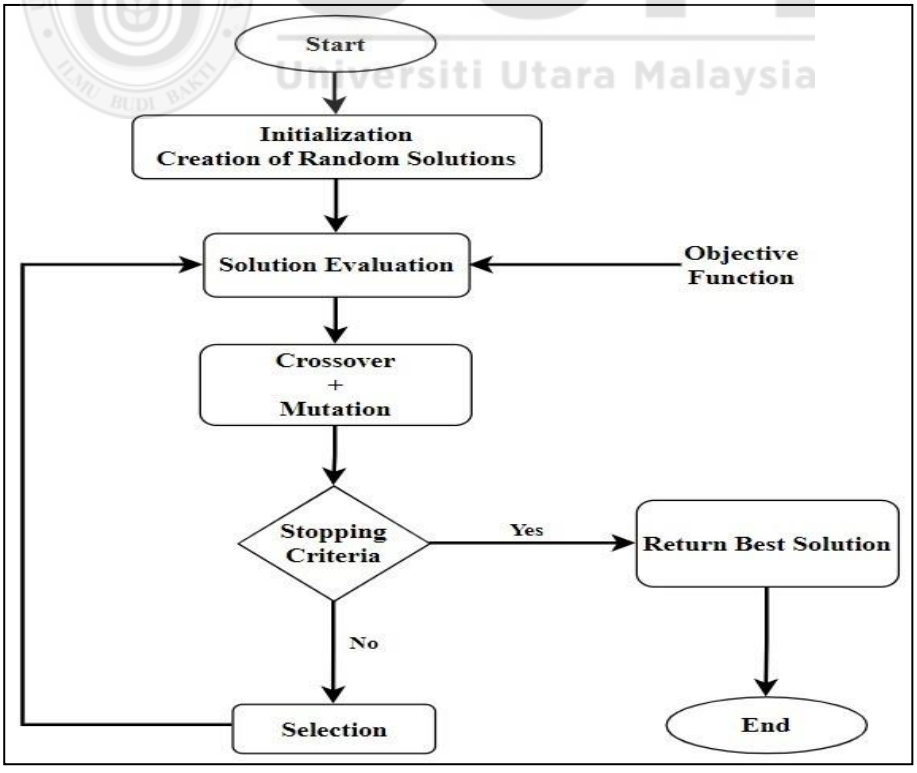


Figure 4.5 Flowchart for Genetic Searching Based on Single Decomposition 1-DGA

(ii) Genetic Algorithm for Multiple Decomposition

The algorithm of multiple decomposition-based embedding consists of more than one genetic. It starts by decomposing the message into n parts according to user preference. Each one searches within a part of the image to find the best configuration within the corresponding part. As pointed out, the second objective is to improve the lack of convergence and address the application's customizability, which provides by a decomposition. To trade-off of effectiveness versus efficiency is done using the number n as a control parameter to increase effectiveness by increasing n or increasing efficiency by decreasing n. The crossover and mutation operations are the same for all sub-algorithms. However, each algorithm has its boundary of the solution space. An algorithm flowchart is shown in Figure 4.6. It starts by enabling the user to enter the number n and the restricted region. Subsequently, it decomposes the message according to n. Next, an iteration loop is implemented to perform n genetic algorithms. Each one is for embedding the related part of the message. After each embedding, the restricted region is updated with the new part used for embedding.

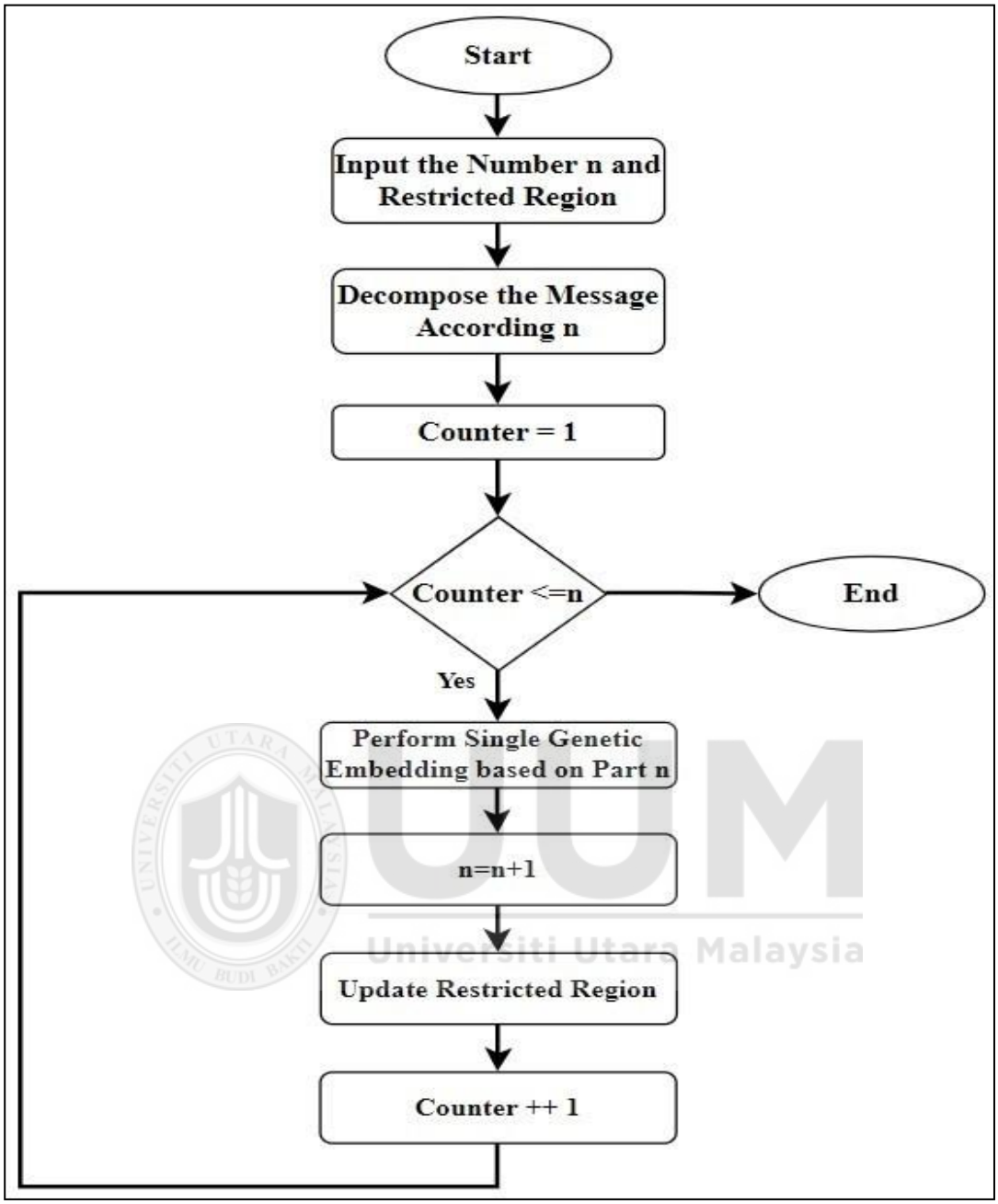


Figure 4.6 Flowchart of Genetic Algorithm for Multiple Decompositions

4.4.3 Embedding based on n-DGA (The Proposed Technique)

A typical steganography scheme consists of two primary stages: embedding and extraction. The embedding algorithm is responsible for inserting the message into a carrier medium such as an image, text, audio, or video. In contrast, the extraction procedure retrieves the embedded message from the host. The procedures of the extraction algorithm are simpler than the

procedures of the embedding algorithm. The greatest difficulty in developing the steganography embedding process is guaranteeing a high imperceptibility of the stego-image.

The LSB technique is one of the traditional steganography techniques; due to its simplicity, high capacity, reasonable distortion of the resulted stego images, and low computational cost, the LSB has been utilized in most information-hiding techniques. Nonetheless, the LSB technique has numerous limitations, such as not distinguishing between high-contrast and smooth areas, which greatly simplifies the steganalysis process (Shanthakumari et al., 2021; Hussain et al., 2018). The LSB technique conceals the message bits sequentially or randomly within the image pixels (Kamau, 2014; Rodrigues et al., 2004). When sequential selection is used, a path is created to replace the LSBs of the image pixels with the secret message bits. A pseudo-random number generator (PRNG) is required for random selection. The numbers resulting from the PRNG specify the specific bits of the host image pixels to hide the secret message parts. The random selection of the traditional LSB technique is more secure than the sequential selection because the numbers generated by the PRNG are saved as a stego key, thus protecting confidential data from unauthorized extraction (Kasapbas & Elmasry, 2018; Khalind & Aziz, 2015).

In the proposed method, the embedding process in Algorithm 4.3 is presented. The input contains three variables: image, message, and control parameter (n). The algorithm starts with decomposing the message into n parts, so there will be n subspaces to find the optimal location to embed the message. Next, it conducts a loop to call the genetic algorithm with n times, each producing the best solution (chromosome). Then, the message part is embedded into the host image pixels depending on the number and positions of the bit-plane LSBs determined in the best solution (best chromosome).

Algorithm 4.3: Embedding Process

```
Input
   Image, Message
   n                          %% controlling parameter
Output
  Stego-Image
  longChromosome          %% Stego-key
Start
   Portions=Decompose (Message,N)
   longChromosome=[];
   For n=1 until N
      [bestChromosome,Image]=Call genetic for Portion(n) to embed in Image
      add bestChromosome to longChromosome
 end
  return Stego-Image, longChromosome
End
```

Based on Algorithm 4.3, the stego-key is generated from the best chromosome for each part. Single chromosomes are sequenced to generate the final stego-key. Thus, the stego-key includes the chromosomes generated from each part in the same message input sequence, ensuring that the retrieved message matches the embedded message. Hence, the outputs of the embedding algorithm are the stego-image and the stego-key, which are the input to the extraction algorithm.

4.5 Extraction Process Stage

The primary objective of the extracting stage is to retrieve the embedded data (secret message bits) from the image pixels (i.e., LSBs of a pixel) and follow a designed embedding stage's approach. Before the embedding process, most information regarding the extracting Process is exchanged by agreement between the sender and receiver because the extraction process is the inverse of the embedding process. On the side of the sender, who is responsible for embedding the secret message inside the transmission medium (image), the procedures of the embedding

process are recorded and saved as a stego-key which makes the embedding process robust against analyzing attacks, thus making information extraction difficult and computationally useless for hackers. On the receiver side, the person authorized to extract the hidden message from the stego object at the receiving destination is the one who has the stego-key. Stego-key contains important details about steganography within the image.

The extraction process of this proposed technique is based on the best chromosomes generated after optimization. It operates by analyzing them individually and using their code to identify the locations, directions, bits used, numbers, and polarization to extract them correctly. The message bits hidden in the host image are specifically extracted from the bit-planes decision variable according to the information of other variables. These bits are collected and then divided into 7 bits after the other, converted to the ASCII code, and thus to the understandable alphabet. The extraction procedure works according to the pseudocode, as shown in Algorithm 4.4.

Algorithm 4.4: Extraction Process

```
Input
  StegnoImage
  Chromosomes
Output
  Message
Start
Message= [];      % Initiate message as empty
For each chromosome [longChromosome]
    extract embedding information  % direction, X-offset, Y-offset, Bit-Planes, SB-Pole, SB-Dir, BP-Dir
    extract the corresponding portion according to the information
   add to message
end
return message
End
```

4.6 Validation Stage

The validation of the suitability of existing steganography techniques for particular applications is harder since the lack of a typical model that can assess the steganography's performance in those applications. This section is decomposed into two sub-sections. First, tracing tests used for validation are presented in sub-section 4.6.1. Second, the messages parts validation is presented in sub-section 4.6.2, which shows the message parts after embedding.

4.6.1 Tracing Tests

This section provides tracing examples for embedding the following message "Steganography is the practice of concealing a message within another message or a physical object." The validation's role is to ensure that the steganography selects reasonable blocks for inserting the message without damaging the area responsible for the diagnostic. In addition, it aims at validating the convergence curve of the optimization. For this goal, three images from three datasets are used, chest, retinal, and brain. The current validation aims to show that the message will be decomposed into parts and embedded in different places in the image. Figures 4.7 (a), 4.8 (a), and 4.9 (a) show the convergence curve of the fitness, i.e., penalty, function for the embedding to the right and the corresponding embedding blocks to the left for the datasets: Chest, Retina, and Brain, respectively.

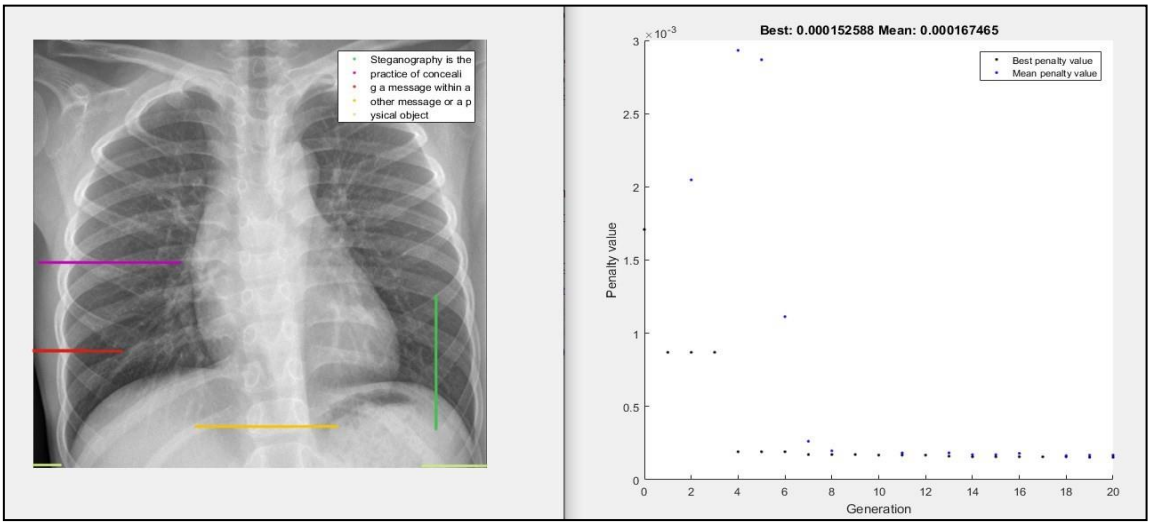


Figure 4.7 (a) The Fitness Convergence Curve and the Corresponding Embedding Blocks in the Chest Dataset

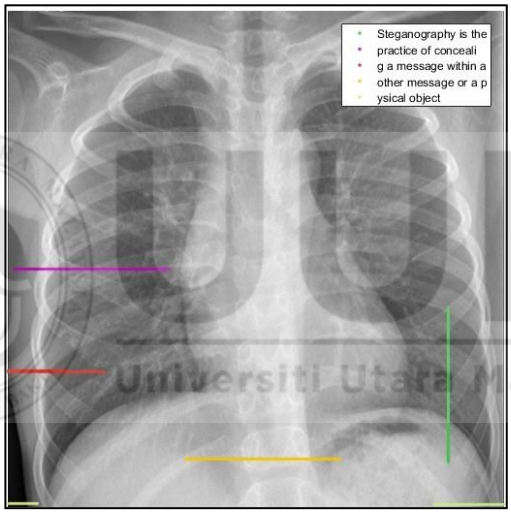


Figure 4.7 (b) The Host Image for the Chest and the Embedding Blocks

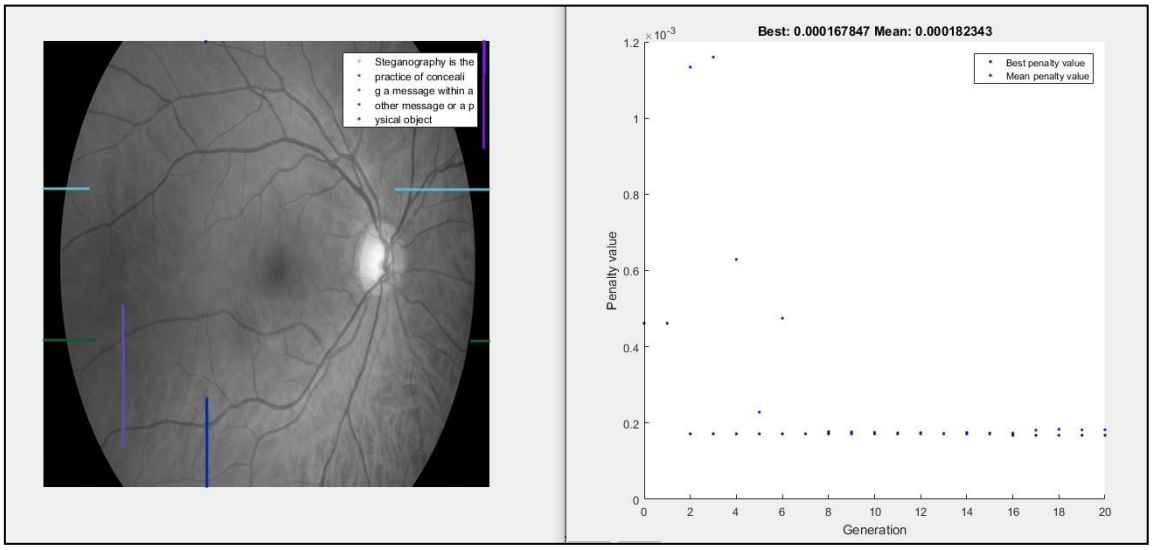


Figure 4.8 (a) The Fitness Convergence Curve and the Corresponding Embedding Blocks in the Retina Dataset

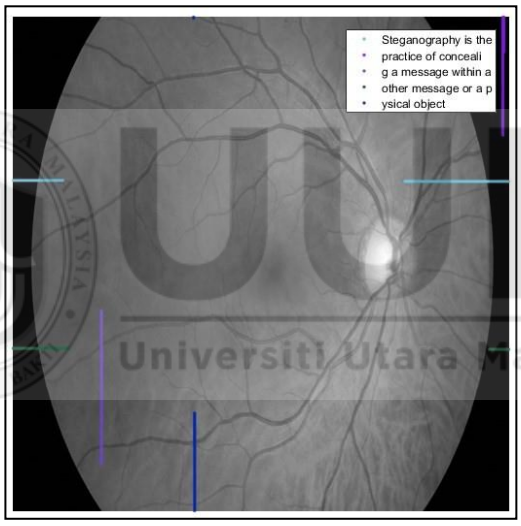


Figure 4.8 (b) The Host Image for the Retina and the Embedding Blocks

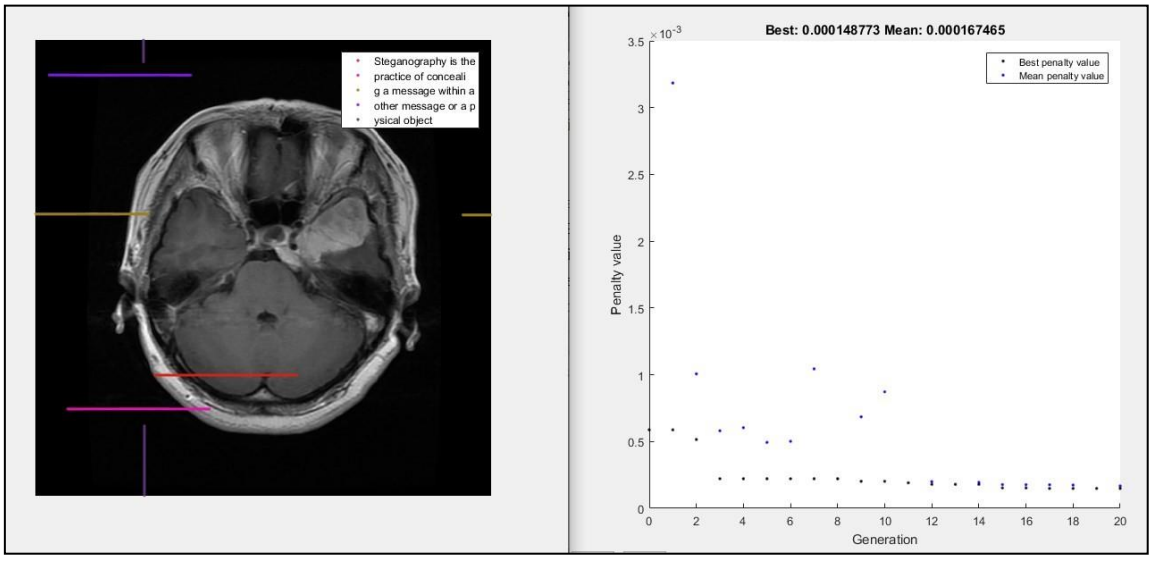


Figure 4.9 (a) The Fitness Convergence Curve and the Corresponding Embedding Blocks in the Brain Dataset

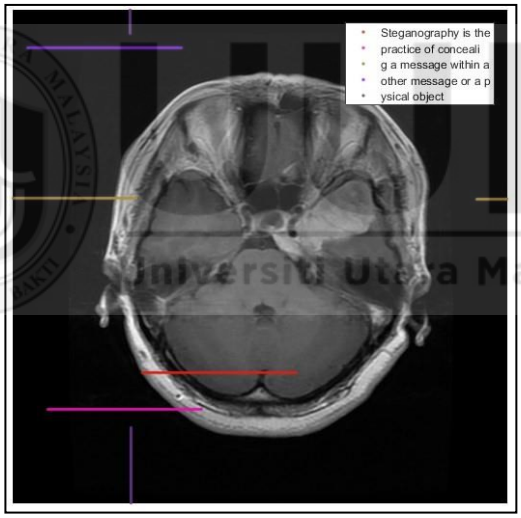


Figure 4.9 (b) The Host Image for the Brain and the Embedding Blocks

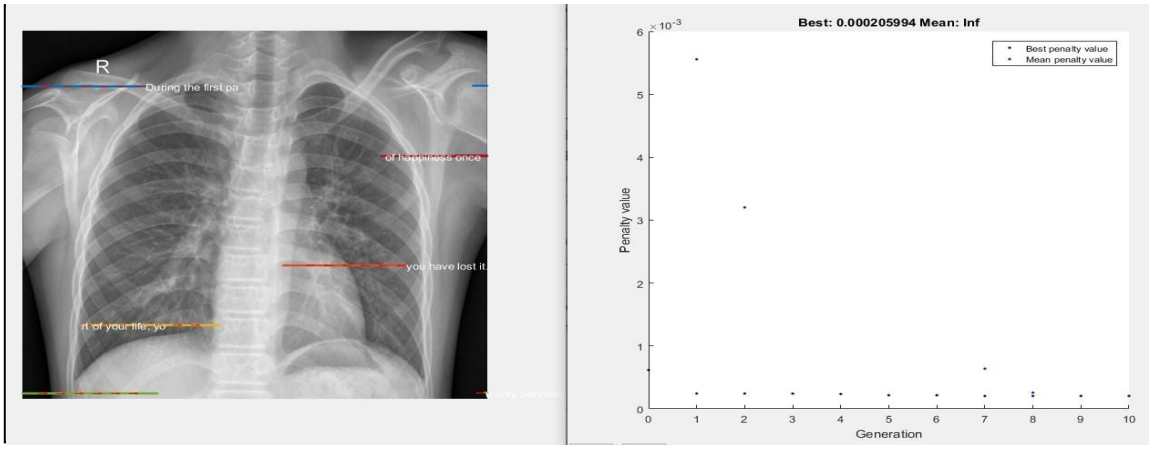
According to Figures 4.7 (a), 4.8 (a), and 4.9 (a), it is found that most of the selected embedding blocks are located in the image's borders. At the same time, the central portion is mostly avoided, which assists in protecting the diagnostic region. The red line in the brain image in Figure 4.9 does not affect the brain's visual information for diagnosis.

Furthermore, it is observed that the algorithm could converge toward a minimum cost function for all three image types, indicating correct optimization behavior. Also, Figures 4.7 (b), 4.8

(b), and 4.9 (b) show the locations and direction of the embedding blocks in the host image. For tracing, the messages embedded in the blocks were marked with different colors for the datasets: Chest, Retina, and Brain, respectively.

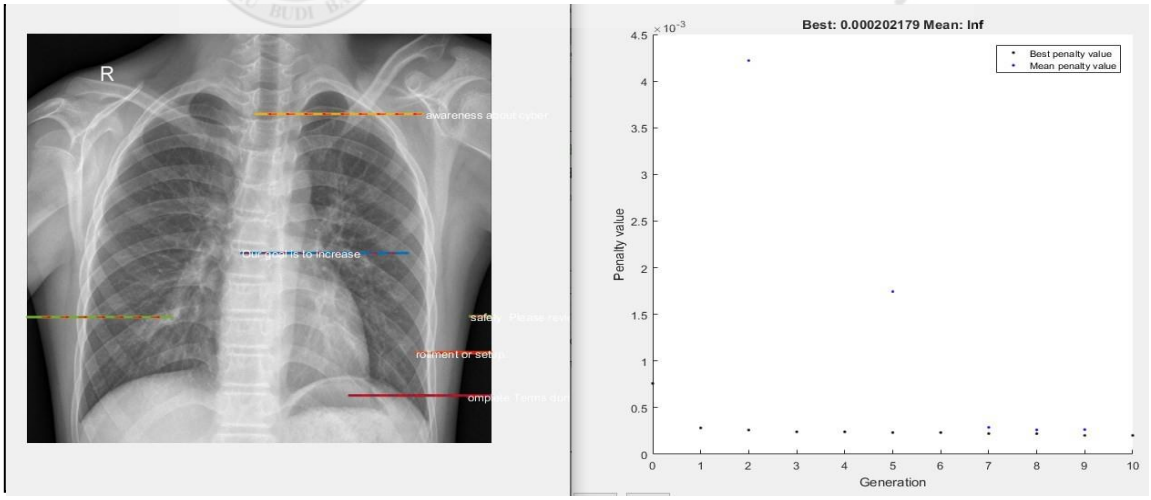
4.6.2 Messages Parts Validation

This section provides further validation by showing blocks with the corresponding message embedded in those blocks. All parts of the secret message, **"Steganography is the practice of concealing a message within another message or a physical object,"** have been inserted in the host image, and no character was lost. The insertion process did not affect the quality of the resulting image (stego-image) for both the Chest and Retina dataset. At the same time, we note the insertion of the message in the Brain dataset, which occurred in locations close to the edges. However, it did not achieve a higher quality than the benchmark technique, and the reason for this is likely because the brain images contain wide dark places.



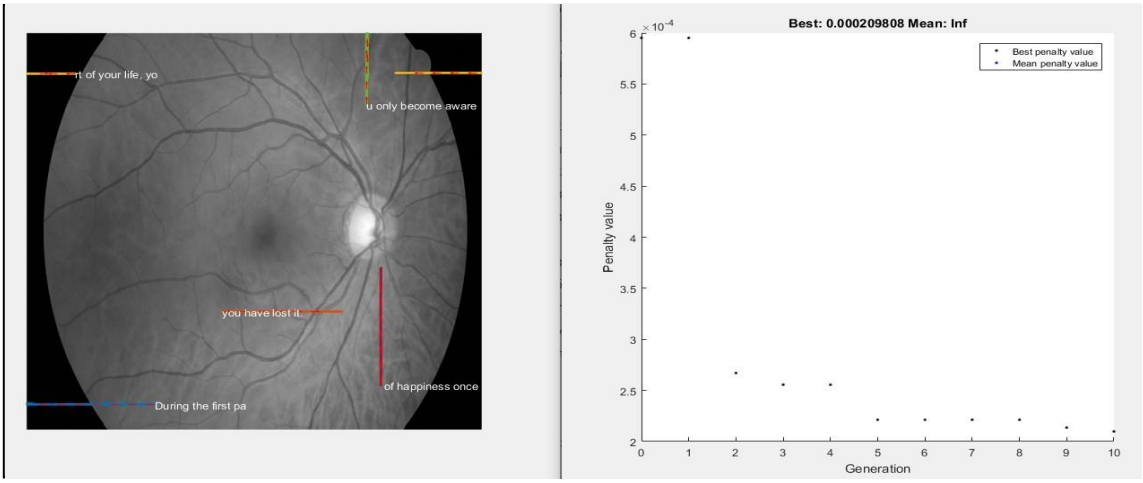
(a)

(b)



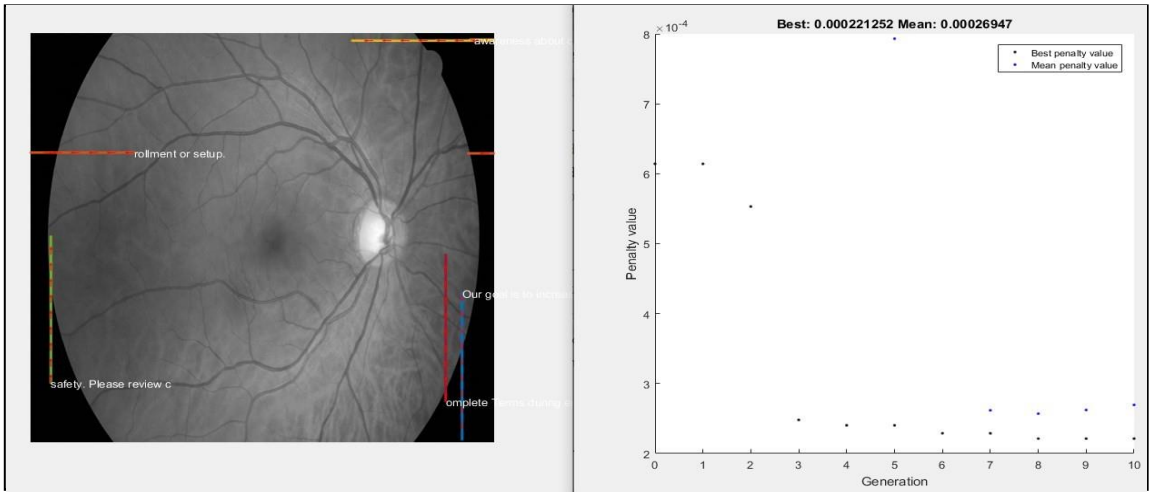
(c)

Figure 4. 10 (a, b, and c) Message Parts Validation After Embedding and the Direction for the Chest Dataset and the Corresponding Convergence Curve



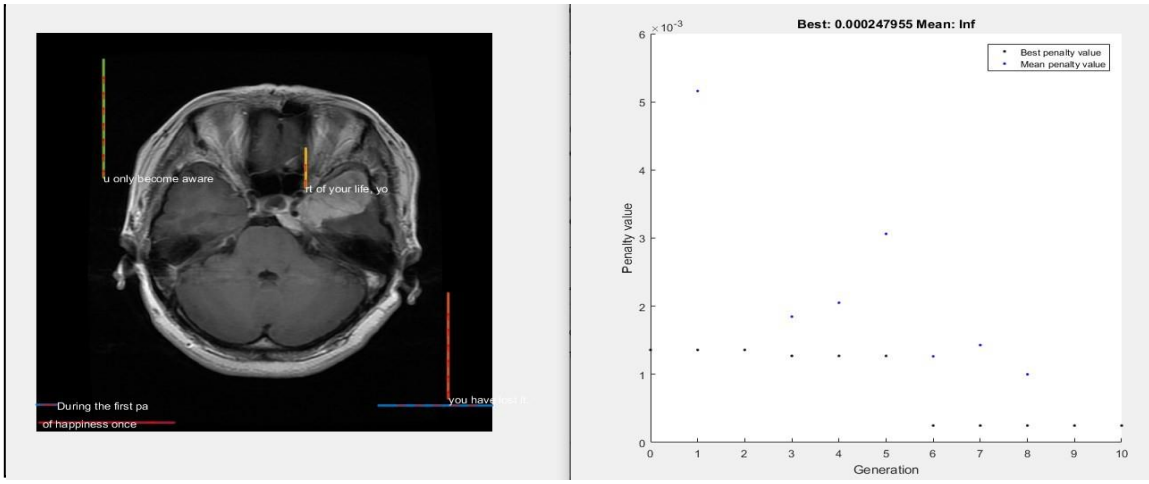
(a)

(b)



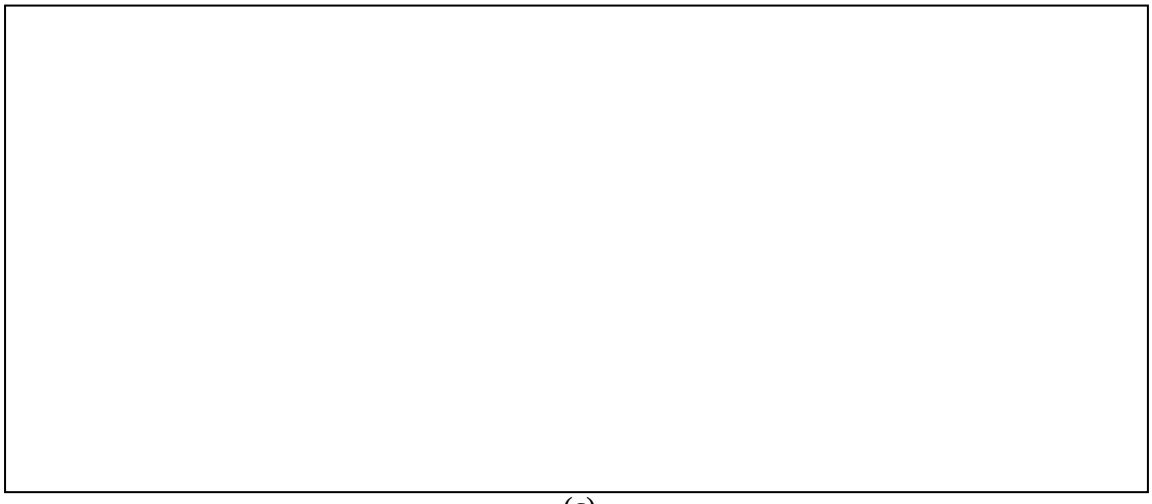
(c)

Figure 4. 11 (a, b, and c) Message Parts Validation After Embedding and the Direction for the Retina Dataset and the Corresponding Convergence Curve



(a)

(b)



(c)

Figure 4. 12 (a, b, and c) Message Parts Validation After Embedding and the Direction for the Brain Dataset and the Corresponding Convergence Curve

As shown in Figures 4.10 (a, b, and c) and 4.11 (a, b, and c), and 4.12 (a, b, and c), examples of hidden information in the datasets are Chest, Retina, and Brain, respectively. The figures above show the embedding direction in each block, which does not follow a unique direction but changes from one image to another and one block to block.

4.7 Summary

To retain the imperceptibility and high security of the sensitive data embedded in the steganography scheme, the proposed n-DGA method for concealing secret data in a medical image was introduced in this chapter. The proposed n-DGA utilized three major stages: data preparation, including image and message preprocessing, embedding, and extraction. Furthermore, three datasets—namely, the Chest, Retina, and Brain—were used to confirm the display of the steganography using n-DGA. Three significant procedures were used to ensure the security and imperceptibility of the suggested steganography scheme. The first is dividing the solution space by dividing the message into n parts, and the second is identifying decision variables and constraints. The third is using a genetic algorithm to search for the best solutions for all parts of the solution space. The proposed embedding method distributes the message in different unconnected locations. Each part of the message has a solution space where the genetic algorithm searches for the best possible solution. The optimal solutions may differ from one part to another. The sum of these solutions is the stego key, with the help of which the recipient can extract confidential information.

In the previous section, a showing of the message embedded in the host image was performed. The observation is that the message was dividable into various blocks according to the number n, and the embedding occurred in various blocks in the image. It is observed that two main types of blocks have resulted, namely, horizontal and vertical. Furthermore, the blocks have

not concealed critical information about the diagnosis, making the algorithm safe to apply in the medical image.

Also, the observation has shown two types of information: the optimization's convergence curve and the resulting blocks from the optimization with the corresponding parts from the message embedded. It has shown that the algorithm has converged to an optimal fitness value, and the blocks were placed in locations that do not conceal the image information required for diagnosis. Thus, distributing the secret message in different unconnected parts enhances security. The final scheme withstood the most common attacks utilized in image steganography systems to achieve the desired results compared to previous work, which proved that the proposed method is better at medical image steganography than the state-of-the-art. The next chapter presents more detailed information on the evaluation of n-DGA and its comparison with the benchmarks.

CHAPTER FIVE
EVALUATION AND ANALYSIS

5.1. Introduction

Steganography is a technique for transferring secret information (such as text) from the sender (source) to the received (destination) via a medium (for example, an image). In information hiding, the communication network between two parties via a far distance is generally evaluated based on two main requirements: imperceptibility and security. Steganography systems, to be reliable, must consider the appropriate evaluation metrics. This chapter evaluates the proposed technique and compares it with state-of-the-art algorithms. Hence, this chapter provides the experimental results and analysis for both the proposed technique and the benchmarks. It starts with the experimental results and analysis provided in Section 5.2. Next, the summary and conclusion are provided in Sections 5.3 and 5.4, respectively.

5.2. Experimental Results and Analysis

Due to the exponential growth in the communications network and people's growing passion for new technologies, computer scientists and security analysts have recently realized the security risks posed by steganography techniques in the global information space. This prompted them to increase their efforts to develop intelligent algorithms to hide sensitive data (Rao et al., 2021; Taha et al., 2019). For example, but not limited to, terrorists can use steganography to communicate secretly without the knowledge of law enforcement agencies. Also, unauthorized persons can tamper with essential and confidential information for a purpose. As a result, studies have continued to look for problems with existing steganography systems that can be exploited to reveal, extract and destroy confidential information.

There are two main approaches to steganography analysis; the first is a visual analysis which is not considered in this thesis. The objective of this approach is to detect the existence of information that is concealed by the naked eye or computer-aided investigation. The second is statistical analysis; steganography systems that utilize statistical analysis to detect the presence of confidential messages in an object are called stego-steganalysis (Provos & Honeyman, 2003). The statistical analysis attempts to detect minor modifications in the hosts (i.e., to reveal statistical features resulting from the steganographic embedding using mathematical theories) (Thabit et al., 2021).

Evaluating the performance of the proposed image steganography scheme in this thesis is based on two essential requirements: imperceptibility and security. This section is divided into two sub-sections; sub-section 5.2.1 is dedicated to imperceptibility, while sub-section 5.2.2 is devoted to security.

5.2.1 Imperceptibility

In image processing applications, evaluating and measuring the imperceptibility of digital images are still significant issues. The main feature of any information hiding system is to conceal the secret bits within a digital image to remain undetectable by the naked human eye or statistical analysis. The stego-image must not contain any distortions detected for security reasons. Furthermore, under all possible conditions, the resulting stego-image should look identical to the original image. In this research, five experiments were conducted on each image for three datasets: the Chest, Retina, and Brain, to capture the statistical performance. Evaluating the imperceptibility was through differences and similarities between original and stego images, various metrics such as Mean Squared Error (MSE), Peak-Signal-to-Noise Ratio (PSNR), and Correlation were used.

Firstly, the MSE measured the mean square of the error in intensity values between the original and stego images, i.e., the statistical difference in pixel values were estimated based on Equation 3.3. Secondly, for calculating the similarity between the stego-image and the host, the PSNR and Correlation have been utilized on Equations 3.4 and 3.5, respectively. Stego-image quality analysis is based on these parameters for the Chest, Retina, and Brain dataset of n-DGA algorithms and compared them with the benchmark, where n changes from 2 to 10. A table presents the numerical results for ten images for each dataset, respectively. Each image's results are listed in a single row in the table.

(i) Chest Dataset

A set of Chest images were selected from a dataset provided by Kaggle using the URL (https://www.kaggle.com/datasets/paultimothymooney/Chest-xray-pneumonia). These images are examples of common use in medical diagnosis; these images were used in the proposed technique for experimental purposes as a host to conceal the secret message. The first numerical results are MSE which has been computed by Equation 3.3. The MSE determines the image quality; for optimum image quality, MSE should be kept to a bare minimum. For the Chest dataset, the value of MSE has decreased for the first image from 0.0582 to 0.0560 compared with the value of 0.0587 for the benchmark, as shown in Table 5.1. A similar observation is found for the remaining set of images. Figure 5.1 illustrates a graphical representation of the comparison outcomes.

Table 5.1

MSE results for n-DGA and comparison to the benchmark

Image-No	Benchmark	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.0587	0.0582	0.0577	0.0573	0.0570	0.0570	0.0566	0.0566	0.0564	0.0560
2	0.0583	0.0580	0.0576	0.0574	0.0571	0.0569	0.0565	0.0567	0.0565	0.0558
3	0.0586	0.0579	0.0577	0.0575	0.0571	0.0571	0.0564	0.0562	0.0561	0.0560
4	0.0585	0.0581	0.0577	0.0575	0.0568	0.0569	0.0566	0.0564	0.0564	0.0560
5	0.0588	0.0580	0.0577	0.0572	0.0572	0.0567	0.0565	0.0565	0.0562	0.0561
6	0.0580	0.0577	0.0573	0.0572	0.0565	0.0562	0.0561	0.0560	0.0561	0.0558
7	0.0576	0.0578	0.0573	0.0569	0.0565	0.0566	0.0562	0.0563	0.0558	0.0555
8	0.0577	0.0572	0.0574	0.0568	0.0568	0.0562	0.0560	0.0564	0.0556	0.0557
9	0.0578	0.0578	0.0574	0.0571	0.0567	0.0564	0.0560	0.0563	0.0561	0.0551
10	0.0578	0.0574	0.0576	0.0572	0.0568	0.0561	0.0562	0.0561	0.0562	0.0554
Average	**0.0582**	**0.0578**	**0.0575**	**0.0572**	**0.0569**	**0.0566**	**0.0563**	**0.0564**	**0.0561**	**0.0557**

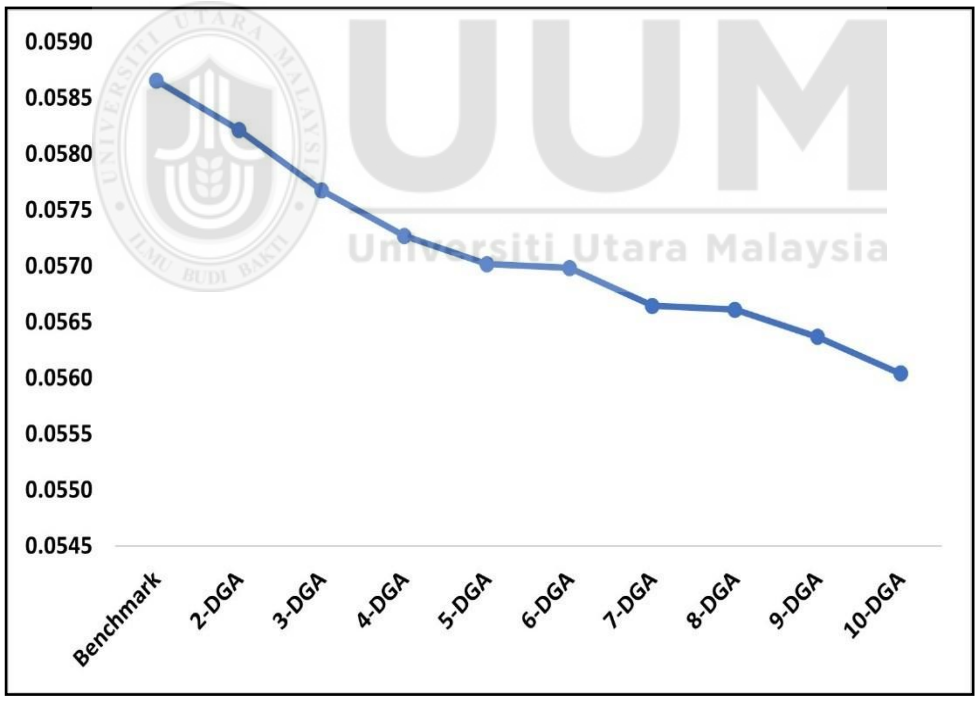


Figure 5.1 MSE Measure for Chest Dataset

Observing Figure 5.1 reveals that the benchmark has generated the highest values of MSE. On the other side, our developed DGA has generated lower values of MSE. Furthermore, increasing the value of n leads to a lower value of MSE. The value of MSE when n=10 is

0.0560, while the value of MSE was around 0.0585 for the benchmark. As a result, the user can use n as a controlling parameter to achieve the desired performance level according to the values provided. This is an attribute of n-DGA as it is accompanied by a degree of freedom to adjust the performance to the desired level. Furthermore, this is interpreted by reducing the solution space from a high-dimensional one in the benchmark to a small one because of the decomposition given in n-DGA.

The improvement in MSE for the Chest dataset is presented in Table 5.2. It is found that 10-DGA has accomplished the highest improvement percentage, which has reached the value of 0.044 for image 1. This improvement indicates n's role when the value is increased in enhancing the quality or effectiveness of the steganography system.

Table 5.2

Improvement of the MSE value for the n-DGA Chest Dataset

Image-No	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.00754	0.01671	0.02367	0.02796	0.02855	0.03434	0.03492	0.03908	0.04461
2	0.00510	0.01177	0.01544	0.02139	0.02394	0.03179	0.02695	0.03146	0.04337
3	0.01243	0.01529	0.02004	0.02687	0.02628	0.03858	0.04177	0.04320	0.04496
4	0.00808	0.01420	0.01753	0.02945	0.02886	0.03258	0.03590	0.03714	0.04391
5	0.01233	0.01804	0.02674	0.02635	0.03446	0.03907	0.03862	0.04394	0.04615
6	0.00572	0.01269	0.01394	0.02605	0.03065	0.03275	0.03512	0.03210	0.03815
7	-0.00378	0.00444	0.01192	0.01848	0.01630	0.02352	0.02213	0.03074	0.03637
8	0.00886	0.00536	0.01442	0.01462	0.02586	0.02864	0.02150	0.03545	0.03453
9	0.00040	0.00660	0.01142	0.01868	0.02501	0.03043	0.02660	0.02957	0.04626
10	0.00844	0.00501	0.01101	0.01734	0.03027	0.02908	0.02968	0.02796	0.04247

The second numerical result is the PSNR computed by Equation 3.4. PSNR is the similarity in image quality between the original image and the stego-image. After embedding the secret message in the original image, a stego-image is produced and may cause some distortions inside it. The embedding process is considered successful and imperceptible to the human eye;

if the PSNR value is between 30 dB and 40 dB, it could be passable, but if the value of PSNR is less than 30 dB is inadmissible because the deformity is very high (Taha et al., 2022; Al-Tamimi & Al-Qobati, 2015). A higher value of PSNR means slight deformity, which is very good if the PSNR value is greater than 40 decibels (dB) (Ranjith Kumar et al., 2016). For the Chest dataset, as shown in Table 5.3, increasing the value of n implies increasing the value of PSNR for n-DGA.

Furthermore, despite the low value of n, the n-DGA obtained a better value of PSNR compared with the benchmark. For example, in image 1, the value of PSNR was for the benchmark 60.4475, while it was for 2-DGA 60.4804. Furthermore, it has increased to 60.6457 when the value of n has increased to 10. A similar observation is found for the remaining set of images. This is interpreted by the small search possibilities compared with the benchmark, even when the decomposition factor n is set to 2. In addition, we observe that the performance is generalizable to all sets of tested images. Hence, the superiority of n-DGA is generalizable. Again, this is interpreted with the fact that n-DGA perform its searching on smaller dimension.

Table 5.3

*PSNR results for n-DGA a*nd comparison to the benchmark

Image-No	Benchmark	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	60.4475	60.4804	60.5207	60.5515	60.5707	60.5733	60.5992	60.6019	60.6206	60.6457
2	60.4727	60.4949	60.5241	60.5403	60.5666	60.5779	60.6130	60.5913	60.6115	60.6652
3	60.4495	60.5038	60.5164	60.5374	60.5678	60.5651	60.6203	60.6348	60.6413	60.6492
4	60.4557	60.4909	60.5178	60.5325	60.5855	60.5829	60.5995	60.6145	60.6200	60.6507
5	60.4390	60.4929	60.5181	60.5567	60.5550	60.5913	60.6121	60.6101	60.6342	60.6442
6	60.4966	60.5215	60.5521	60.5576	60.6112	60.6318	60.6413	60.6519	60.6383	60.6655
7	60.5276	60.5112	60.5469	60.5797	60.6086	60.5989	60.6309	60.6248	60.6632	60.6885
8	60.5210	60.5596	60.5443	60.5840	60.5849	60.6348	60.6472	60.6153	60.6777	60.6736
9	60.5115	60.5132	60.5403	60.5614	60.5934	60.6215	60.6457	60.6286	60.6418	60.7172
10	60.5081	60.5449	60.5299	60.5562	60.5840	60.6416	60.6362	60.6389	60.6312	60.6965
Average	**60.4829**	**60.5113**	**60.5311**	**60.5557**	**60.5828**	**60.6019**	**60.6245**	**60.6212**	**60.6380**	**60.6696**

Figure 5.2 depicts the graphical representation of the PSNR measurement of the chest dataset, comparing the results of the proposed method with the benchmark method.

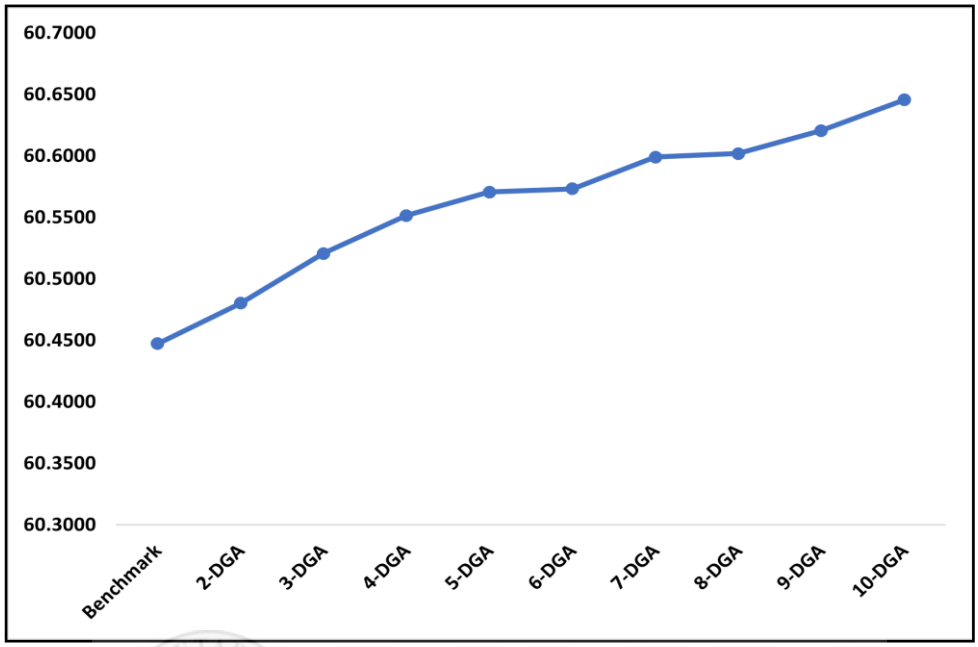


Figure 5.2 PSNR Measure for Chest Dataset

Similar to MSE, the values of PSNR that have been generated for the benchmark is the least 60.4500 compared with the highest value of 60.6500, which is the result of our developed DGA when the value n =10. This provides the superiority of DGA over the benchmark. Furthermore, the curve of PSNR generated from DGA provides values of PSNR ranging between 60.5000 and 60.6500, which provides an acceptable range to control the performance according to user preference.

To analyze the improvement in PSNR for n-DGA compared with the benchmark, presented in Table 5.4. The increasing value of n implies more improvement of n-DGA than the benchmark. However, the improvement percentage of PSNR has reached its maximum value of 0.003 compared with the benchmark. Furthermore, it is lower than the improvement in terms of MSE because PSNR is a normalized performance metric.

Table 5.4

Improvement of the PSNR value for the n-DGA Chest Dataset

Image-No	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.0005	0.0012	0.0017	0.0020	0.0021	0.0025	0.0026	0.0029	0.0033
2	0.0004	0.0009	0.0011	0.0016	0.0017	0.0023	0.0020	0.0023	0.0032
3	0.0009	0.0011	0.0015	0.0020	0.0019	0.0028	0.0031	0.0032	0.0033
4	0.0006	0.0010	0.0013	0.0021	0.0021	0.0024	0.0026	0.0027	0.0032
5	0.0009	0.0013	0.0019	0.0019	0.0025	0.0029	0.0028	0.0032	0.0034
6	0.0004	0.0009	0.0010	0.0019	0.0022	0.0024	0.0026	0.0023	0.0028
7	-0.0003	0.0003	0.0009	0.0013	0.0012	0.0017	0.0016	0.0022	0.0027
8	0.0006	0.0004	0.0010	0.0011	0.0019	0.0021	0.0016	0.0026	0.0025
9	0.0000	0.0005	0.0008	0.0014	0.0018	0.0022	0.0019	0.0022	0.0034
10	0.0006	0.0004	0.0008	0.0013	0.0022	0.0021	0.0022	0.0020	0.0031

The third numerical result is the Correlation (r) computed by Equation 3.5. A correlation is a metric that indicates the similarity between the original image and the stego-image, which is a significant characteristic. Generally, an individually bit plane in an image correlates with its neighbors. The Correlation may be altered after employing the embedding technique, which can be detected using bit plane analysis. For the Chest dataset, as shown in Table 5.5. The value (r) has increased from 0.999989535 for 2-DGA to 0.999989926 for 10-DGA compared with only 0.999989457 for the benchmark in image 1. Similar results in other images confirm the correlation n-DGA superiority over the benchmark.

Table 5.5

*Correlation results for n-DGA a*nd comparison to the benchmark

Image-No	Benchmark	2-DGA	3-DGA	4-DGA	5-DGA	6-DGA	7-DGA	8-DGA	9-DGA	10-DGA
1	0.999989457	0.999989535	0.999989635	0.999989704	0.99998975	0.999989757	0.999989816	0.999989822	0.999989867	0.999989926
2	0.999989517	0.999989571	0.999989642	0.999989676	0.999989739	0.999989766	0.999989852	0.999989797	0.999989844	0.999989971
3	0.999989464	0.99998959	0.99998962	0.999989672	0.999989743	0.999989735	0.999989866	0.999989899	0.999989914	0.999989933
4	0.999989476	0.999989559	0.999989625	0.999989659	0.999989784	0.999989779	0.999989816	0.999989851	0.999989864	0.999989936
5	0.999989435	0.999989566	0.999989626	0.999989717	0.999989715	0.999989797	0.999989845	0.999989841	0.999989898	0.99998992
6	0.999989914	0.999989967	0.999990038	0.99999005	0.999990171	0.999990216	0.999990237	0.999990262	0.999990232	0.999990292
7	0.999989984	0.999989943	0.999990023	0.999990099	0.999990165	0.999990141	0.999990214	0.999990201	0.999990288	0.999990344
8	0.999989969	0.999990052	0.999990017	0.999990108	0.99999011	0.999990223	0.999990251	0.999990179	0.99999032	0.999990312
9	0.999989956	0.999989953	0.999990009	0.999990057	0.999990129	0.999990195	0.99999025	0.99999021	0.999990238	0.999990408
10	0.999989939	0.999990022	0.999989988	0.999990044	0.999990108	0.999990239	0.999990227	0.999990232	0.999990216	0.999990361
Average	**0.999989711**	**0.999989776**	**0.999989822**	**0.999989879**	**0.999989941**	**0.999989985**	**0.999990038**	**0.999990029**	**0.999990068**	**0.99999014**

Figure 5.3 is a graphical representation of the correlation measurement of the chest dataset, comparing the results of the proposed method with those of the benchmark method.

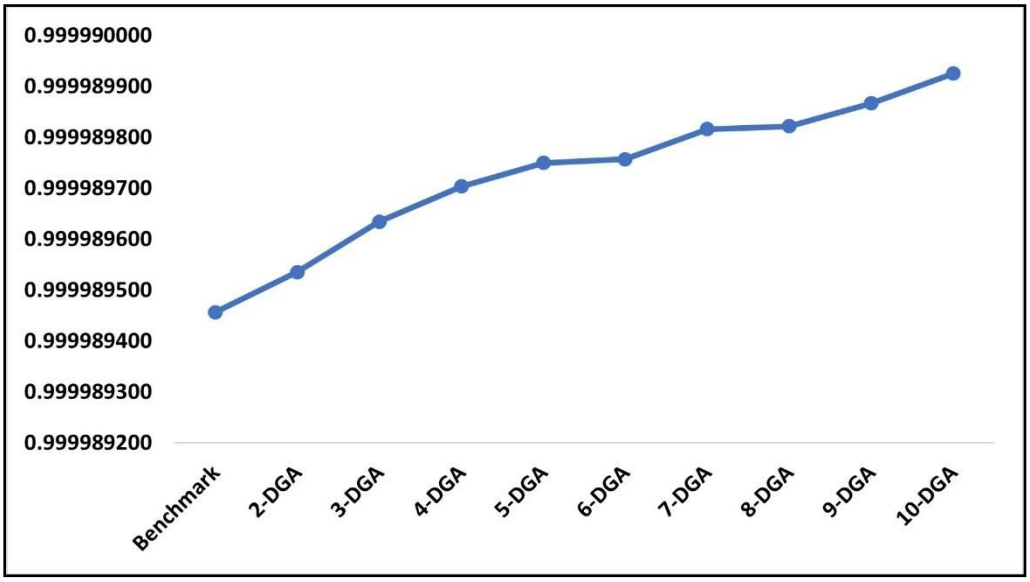


Figure 5.3 Correlation Measure for Chest Dataset

The correlation measure values in Figure 5.3 indicate that 10-DGA has achieved the highest correlation of values compared to the minimum values generated by the benchmark. Again, this demonstrates DGA's superiority over the benchmark. This is interpreted by the fact that n-DGA divides the image into blocks and performs the search on each block separately. Hence, it has more chance to escape from local minima than the benchmark, which means higher correlation values between the original image and the stego-image.

Similar to MSE and PSNR, the improvement percentage in Correlation is present in Table 5.6. It is also observed that increasing the value of n implies more improvement over the Correlation, which had reached the value of 4.68757E-07 for image one and n equaled ten compared with only 7.84802E-08 for the same image when the value of n was two.

Table 5.6

Improvement of the Correlation value for the n-DGA Chest Dataset

Image-No	2-DGA	3-DGA	4-DGA	5-DGA	6-DGA	7-DGA	8-DGA	9-DGA	10-DGA
1	7.84802E-08	1.78007E-07	2.47183E-07	2.92871E-07	3.00272E-07	3.59341E-07	3.65167E-07	4.10228E-07	4.68757E-07
2	5.36006E-08	1.24279E-07	1.58925E-07	2.2112E-07	2.48181E-07	3.34911E-07	2.79401E-07	3.26957E-07	4.53477E-07
3	1.25928E-07	1.55996E-07	2.08109E-07	2.78719E-07	2.71261E-07	4.02293E-07	4.34792E-07	4.49908E-07	4.69136E-07
4	8.29525E-08	1.49249E-07	1.82569E-07	3.07863E-07	3.02324E-07	3.39995E-07	3.75161E-07	3.88068E-07	4.59796E-07
5	1.30714E-07	1.90868E-07	2.81149E-07	2.79764E-07	3.61779E-07	4.10074E-07	4.05501E-07	4.62373E-07	4.84951E-07
6	5.33042E-08	1.24194E-07	1.36187E-07	2.5716E-07	3.02148E-07	3.23615E-07	3.47816E-07	3.17888E-07	3.78358E-07
7	-4.07534E-08	3.89265E-08	1.15179E-07	1.81634E-07	1.5765E-07	2.30077E-07	2.17229E-07	3.04332E-07	3.59868E-07
8	8.32259E-08	4.87113E-08	1.3923E-07	1.414E-07	2.53845E-07	2.82233E-07	2.10602E-07	3.50961E-07	3.43422E-07
9	-3.3627E-09	5.34236E-08	1.01092E-07	1.73568E-07	2.39473E-07	2.94298E-07	2.54635E-07	2.82437E-07	4.51685E-07
10	8.34311E-08	4.87409E-08	1.05294E-07	1.68847E-07	2.99995E-07	2.87743E-07	2.92665E-07	2.77017E-07	4.217E-07

Observing the median value of each n-DGA and the benchmark found that the median of MSE decreases when n increases, which means that n reduces the dissimilarity between the host image and the stego image. As shown in Figure 5.4, all n-DGA configurations have outperformed the benchmark regarding MSE, PSNR, and Correlation. The same observation is revealed for both PSNR and Correlation.

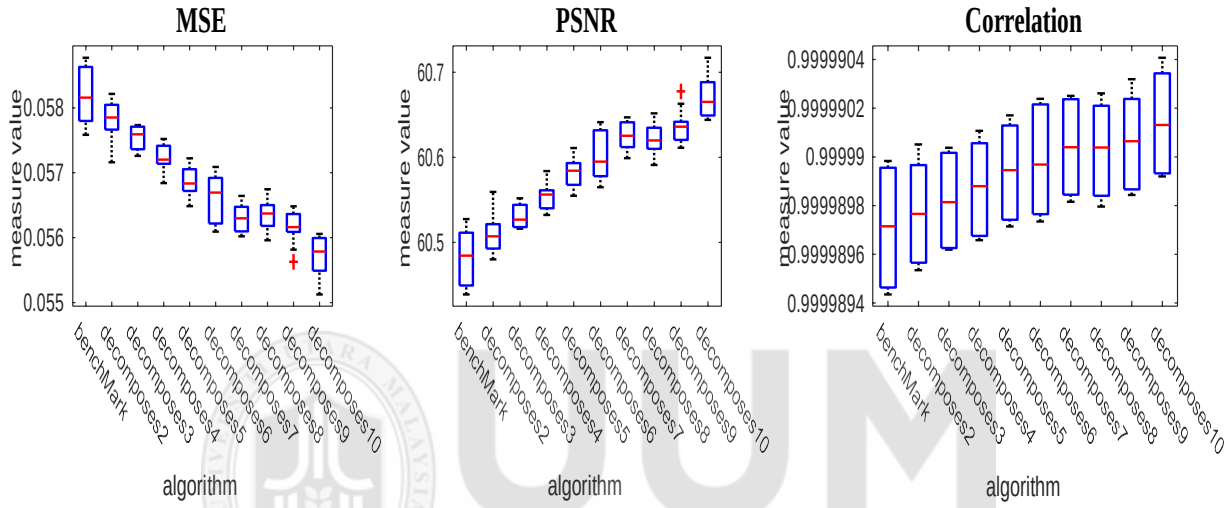


Figure 5.4 Imperceptibility evaluation metrics for n-DGA and its comparison with the benchmark for the Chest dataset

(ii) Retina Dataset

Retina images were selected from a dataset provided by the URL https://www5.cs.fau.de/research/data/fundus-images. These images are examples of common use in medical diagnosis; these images were used in the proposed technique for experimental purposes as a host to conceal the secret message. Similarly, the Retina dataset presented the numerical values of MSE, which have been computed by Equation 3.3. As shown in Table 5.7, MSE has decreased from 0.0567 to 0.0546 for the first image, compared to 0.0570 for the benchmark. The remaining set of images elicits a similar observation.

Table 5.7

*MSE results for n-DGA a*nd comparison to the benchmark

Image No	Benchmark	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.0570	0.0567	0.0566	0.0564	0.0560	0.0556	0.0555	0.0558	0.0555	0.0546
2	0.0566	0.0565	0.0566	0.0563	0.0558	0.0554	0.0555	0.0556	0.0557	0.0544
3	0.0570	0.0569	0.0562	0.0565	0.0561	0.0561	0.0558	0.0554	0.0553	0.0551
4	0.0570	0.0571	0.0564	0.0562	0.0560	0.0555	0.0558	0.0557	0.0553	0.0546
5	0.0571	0.0568	0.0564	0.0560	0.0559	0.0554	0.0557	0.0563	0.0559	0.0549
6	0.0572	0.0565	0.0566	0.0571	0.0562	0.0558	0.0560	0.0557	0.0559	0.0555
7	0.0573	0.0568	0.0566	0.0564	0.0565	0.0559	0.0559	0.0556	0.0561	0.0553
8	0.0573	0.0571	0.0570	0.0567	0.0564	0.0560	0.0561	0.0563	0.0555	0.0551
9	0.0573	0.0570	0.0568	0.0566	0.0567	0.0558	0.0558	0.0560	0.0556	0.0549
10	0.0572	0.0570	0.0568	0.0566	0.0566	0.0560	0.0559	0.0559	0.0555	0.0554
Average	**0.0571**	**0.0568**	**0.0566**	**0.0565**	**0.0562**	**0.0558**	**0.0558**	**0.0558**	**0.0556**	**0.0550**

Similarly, for the chest data set, Figure 5.5 depicts the graphical representation of the MSE measurement of the retina dataset in which the results of the proposed method are compared to the results of the benchmark method.

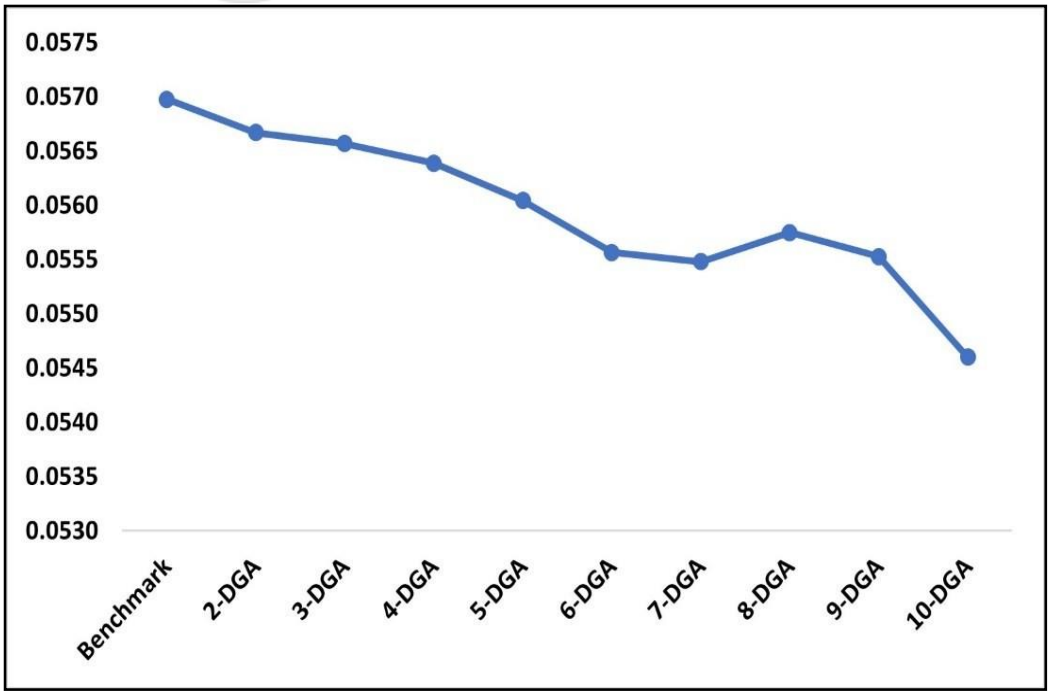


Figure 5.5 MSE Measure for Retina Dataset

Figure 5.5 demonstrates that the MSE values produced by the benchmark were the highest. In contrast, the MSE values generated by our developed DGA are lower. In addition, we observe that as n increases, the MSE decreases. The MSE value for n = 10 ranges from 0.0545 to 0.0550, whereas the MSE value for the benchmark was approximately 0.0570. As a result, the user can use n as a controlling parameter to achieve the desired level of performance based on the values provided for the MSE metric. Same as to the chest dataset, this is an attribute of the n-DGA technique as a result of the degree of freedom in adjusting the control parameter to achieve the desired level of performance. Furthermore, reducing the space of solutions from a high-dimensional space in the benchmark to a small one due to the decomposition given in n-DGA explains the n-DGA technique's superiority.

To illustrate the improvement in MSE for the Retina dataset, Table 5.8 was presented. It was discovered that 10-DGA achieved the highest improvement percentage, reaching 0.041 for image 1. This improvement indicates n's role when the value is increased to improve the steganography system's quality or effectiveness.

Table 5.8

Improvement of the MSE value for the n-DGA Retina Dataset

Image-No	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.0054	0.0072	0.0104	0.0164	0.0248	0.0263	0.0216	0.0254	0.0417
2	0.0033	0.0001	0.0059	0.0149	0.0213	0.0198	0.0188	0.0176	0.0393
3	0.0025	0.0138	0.0095	0.0163	0.0153	0.0218	0.0284	0.0296	0.0340
4	-0.0009	0.0097	0.0137	0.0167	0.0260	0.0207	0.0233	0.0298	0.0430
5	0.0047	0.0118	0.0192	0.0205	0.0292	0.0235	0.0139	0.0211	0.0376
6	0.0128	0.0104	0.0024	0.0171	0.0241	0.0211	0.0258	0.0228	0.0289
7	0.0079	0.0117	0.0151	0.0140	0.0240	0.0248	0.0292	0.0202	0.0348
8	0.0046	0.0063	0.0112	0.0154	0.0231	0.0219	0.0180	0.0320	0.0387
9	0.0045	0.0080	0.0120	0.0093	0.0252	0.0264	0.0216	0.0298	0.0408
10	0.0032	0.0072	0.0103	0.0105	0.0209	0.0229	0.0236	0.0296	0.0317

The PSNR values are presented numerically for the Retina dataset, similar to the Chest dataset, computed by Equation 3.4. As illustrated in Table 5.9, increasing n implies increasing the PSNR for n-DGA. Additionally, despite the low value of n, it achieved a higher PSNR for n-DGA than the benchmark. For instance, in image 1, the PSNR value for the benchmark was 60.5736, while the value for 2-DGA was 60.5972. Additionally, it increased to 60.7586 when n was increased to 10. When the decomposition parameter n is greater than 1, dividing the search space into smaller parts according to the n value provides a small set of search possibilities compared to the standard. Furthermore, we can see that the performance is generalizable across all images tested. The explanation for the superiority of n-DGA is due to the attribute of the technique, the search for the best solution for the small dimensions.

Table 5.9

*PSNR results for n-DGA a*nd comparison to the benchmark

Image No	Benchmark	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	60.5736	60.5972	60.6048	60.6189	60.6454	60.6825	60.6894	60.6682	60.6855	60.7586
2	60.5989	60.6133	60.5992	60.6248	60.6641	60.6927	60.6858	60.6813	60.6759	60.7729
3	60.5710	60.5817	60.6312	60.6124	60.6424	60.6377	60.6667	60.6959	60.7016	60.7211
4	60.5721	60.5680	60.6145	60.6318	60.6454	60.6864	60.6629	60.6745	60.7037	60.7628
5	60.5672	60.5875	60.6189	60.6513	60.6569	60.6959	60.6703	60.6280	60.6596	60.7335
6	60.5573	60.6133	60.6027	60.5678	60.6324	60.6632	60.6501	60.6709	60.6575	60.6846
7	60.5501	60.5846	60.6013	60.6162	60.6115	60.6558	60.6593	60.6789	60.6386	60.7040
8	60.5481	60.5680	60.5753	60.5972	60.6153	60.6495	60.6442	60.6271	60.6894	60.7196
9	60.5518	60.5715	60.5867	60.6042	60.5925	60.6629	60.6679	60.6469	60.6834	60.7329
10	60.5567	60.5707	60.5881	60.6019	60.6024	60.6486	60.6575	60.6605	60.6873	60.6965
Average	**60.5647**	**60.5856**	**60.6023**	**60.6126**	**60.6308**	**60.6675**	**60.6654**	**60.6632**	**60.6783**	**60.7287**

Figure 5.6 is a graphical representation of the PSNR measurement of the retina dataset based on a comparison between the proposed method and the standard method.

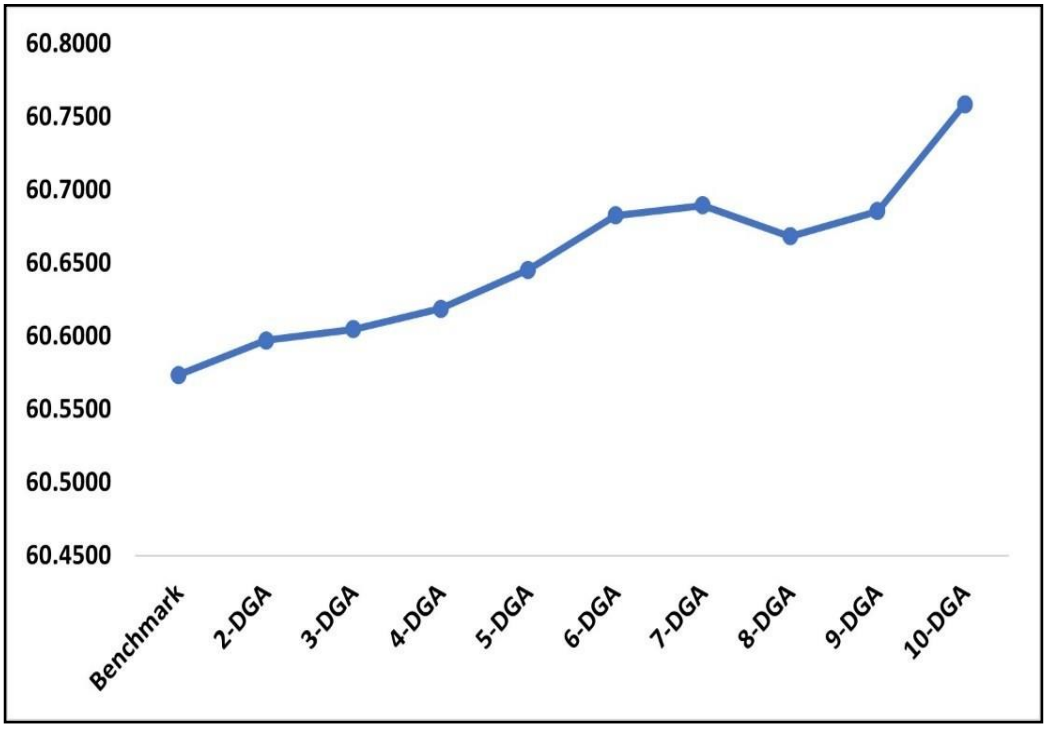


Figure 5.6 PSNR Measure for Retina Dataset

Figure 5.6 demonstrates that the PSNR values of the developed DGA method increased as n increased, as the PSNR at n = 10 ranged between 60.80 and 60.75. This demonstrates that DGA is superior to the benchmark, whose value was between 60.60 and 60.55.

Table 5.10 contains the values for the percentage improvement in PSNR for n-DGA compared to the benchmark for the Retina dataset. The increasing value of n indicates more improvement of n-DGA than the benchmark. However, the percentage improvement in PSNR has reached its maximum value of 0.003 compared to the benchmark, which is less than the percentage improvement in MSE because PSNR is a normalized performance metric.

Table 5.10

Improvement of the PSNR value for the n-DGA Retina Dataset

Image-No	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.0004	0.0005	0.0007	0.0012	0.0018	0.0019	0.0016	0.0018	0.0031
2	0.0002	0.0000	0.0004	0.0011	0.0015	0.0014	0.0014	0.0013	0.0029
3	0.0002	0.0010	0.0007	0.0012	0.0011	0.0016	0.0021	0.0022	0.0025
4	-0.0001	0.0007	0.0010	0.0012	0.0019	0.0015	0.0017	0.0022	0.0031
5	0.0003	0.0009	0.0014	0.0015	0.0021	0.0017	0.0010	0.0015	0.0027
6	0.0009	0.0008	0.0002	0.0012	0.0017	0.0015	0.0019	0.0017	0.0021
7	0.0006	0.0008	0.0011	0.0010	0.0017	0.0018	0.0021	0.0015	0.0025
8	0.0003	0.0005	0.0008	0.0011	0.0017	0.0016	0.0013	0.0023	0.0028
9	0.0003	0.0006	0.0009	0.0007	0.0018	0.0019	0.0016	0.0022	0.0030
10	0.0002	0.0005	0.0007	0.0008	0.0015	0.0017	0.0017	0.0022	0.0023

The third numerical result is the Correlation (r) computed by Equation 3.5. Table 5.11 contains the values of the correlation metric for n-DGA compared with the benchmark for the Retina dataset. The correlation value has increased from 0.999985003 for 2-DGA to 0.999985418 for 10-DGA compared with only 0.999984938 for the benchmark in image 1. Similar results in other images confirm the correlation n-DGA superiority over the benchmark.

Table 5.11

Correlation results for n-DGA *a*nd comparison to the benchmark

Image No	Benchmark	2-DGA	3-DGA	4-DGA	5-DGA	6-DGA	7-DGA	8-DGA	9-DGA	10-DGA
1	0.999984938	0.999985003	0.999984972	0.999985027	0.999985073	0.999985222	0.999985224	0.999985216	0.999985186	0.999985418
2	0.999985048	0.999985097	0.999985006	0.999985042	0.999985209	0.999985276	0.999985292	0.999985223	0.999985065	0.999985498
3	0.999984926	0.999984944	0.999985106	0.99998497	0.999985118	0.999984938	0.999985119	0.999985209	0.999985299	0.999985333
4	0.999984966	0.999984903	0.999985019	0.999985101	0.999985114	0.999985173	0.999985094	0.99998518	0.999985217	0.999985464
5	0.999984914	0.999984964	0.99998508	0.999985218	0.99998513	0.999985305	0.99998515	0.999984907	0.999985011	0.999985312
6	0.999986695	0.999986942	0.999986835	0.999986668	0.999986957	0.999986998	0.99998693	0.999986986	0.999986892	0.999986976
7	0.999986672	0.999986797	0.999986834	0.999986884	0.999986787	0.99998702	0.999986993	0.999987021	0.999986834	0.999987027
8	0.999986743	0.999986709	0.999986779	0.999986767	0.999986864	0.999986896	0.999986909	0.9999868	0.999987022	0.999987106
9	0.999986694	0.999986797	0.999986703	0.999986786	0.999986706	0.999987053	0.999986954	0.999986917	0.999987004	0.999987167
10	0.999986699	0.999986718	0.999986785	0.999986774	0.999986778	0.99998694	0.999986972	0.999986962	0.999987012	0.999987038
Average	**0.999985829**	**0.999985888**	**0.999985912**	**0.999985924**	**0.999985974**	**0.999986082**	**0.999986064**	**0.999986042**	**0.999986054**	**0.999986234**

Figure 5.7 is a graphical representation of the correlation measurement of the retina dataset, in which the results of the proposed method are compared to the results of the benchmark method.

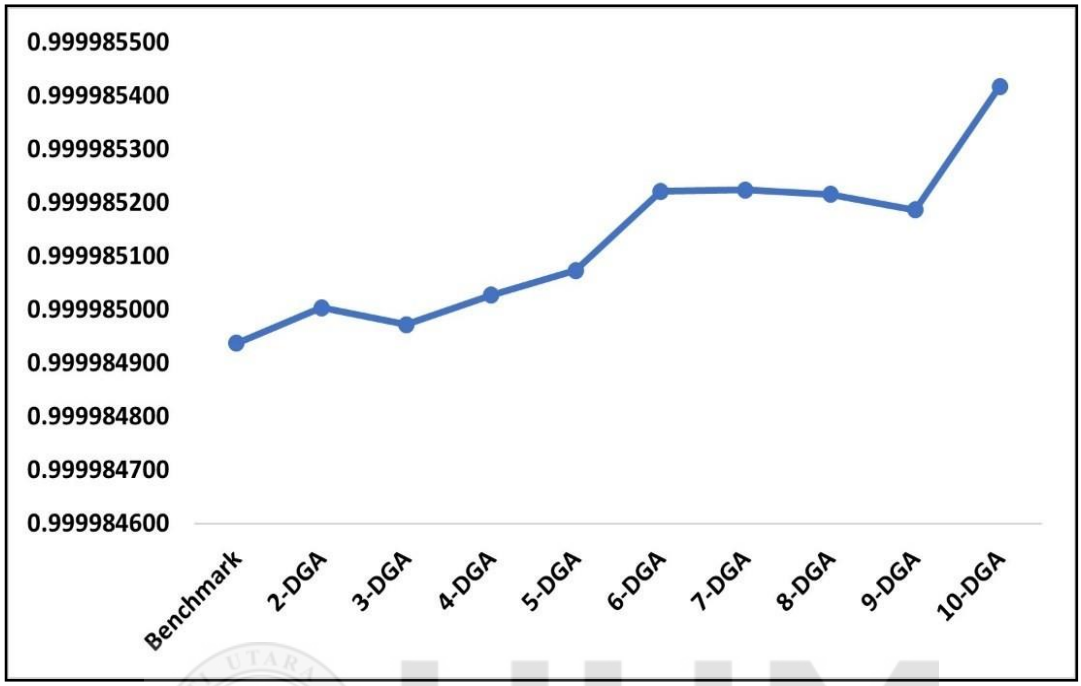


Figure 5.7 Correlation Measure for Retina Dataset

As Figure 5.7, the correlation measure values indicate that 10-DGA has achieved the highest correlation of values relative to the benchmark's minimum values. This indicates the superiority of the developed DGA over the benchmark. The superiority of n-DGA technology is explained by the fact that the image is divided into blocks, and all image blocks are searched separately. As a result, it has a higher chance of escaping from local minima than the benchmark, resulting in higher correlation values between the original image and the stego-image.

The correlation metric's percentage improvement values are presented in Table 5.12. It is observed that increasing the value of n results in a more remarkable improvement in Correlation, which reached 4.8039E-07 for image one when n equals ten, compared to only 6.57885E-08 for the same image when n equals two.

Table 5.12

Improvement of the *Correlation* value for the n-DGA *Retina* Dataset

Image-No	2-DGA	3-DGA	4-DGA	5-DGA	6-DGA	7-DGA	8-DGA	9-DGA	10-DGA
1	6.57885E-08	3.43695E-08	8.94871E-08	1.35525E-07	2.84006E-07	2.86623E-07	2.7809E-07	2.48798E-07	4.8039E-07
2	4.88897E-08	-4.1874E-08	-6.27782E-09	1.61256E-07	2.28219E-07	2.43574E-07	1.75189E-07	1.63779E-08	4.50027E-07
3	1.75534E-08	1.7968E-07	4.34369E-08	1.91351E-07	1.13802E-08	1.92818E-07	2.82301E-07	3.72056E-07	4.06868E-07
4	-6.30173E-08	5.29511E-08	1.3427E-07	1.48002E-07	2.066E-07	1.27741E-07	2.13615E-07	2.50404E-07	4.97744E-07
5	5.00068E-08	1.6643E-07	3.04028E-07	2.16192E-07	3.91534E-07	2.35658E-07	-6.61755E-09	9.75961E-08	3.98078E-07
6	2.47068E-07	1.40347E-07	-2.6825E-08	2.62712E-07	3.03342E-07	2.35033E-07	2.9129E-07	1.97798E-07	2.81014E-07
7	1.25289E-07	1.61951E-07	2.12531E-07	1.15122E-07	3.48162E-07	3.21257E-07	3.49094E-07	1.62022E-07	3.55531E-07
8	-3.40002E-08	3.54087E-08	2.35646E-08	1.20643E-07	1.52898E-07	1.65166E-07	5.62318E-08	2.78552E-07	3.62388E-07
9	1.03348E-07	9.74015E-09	9.27521E-08	1.22893E-08	3.59814E-07	2.60781E-07	2.23966E-07	3.10729E-07	4.73201E-07
10	1.9844E-08	8.66744E-08	7.48712E-08	7.93812E-08	2.41811E-07	2.72916E-07	2.63569E-07	3.12906E-07	3.39215E-07

As Figure 5.8, all n-DGA configurations outperformed the benchmark regarding MSE, PSNR, and Correlation. By comparing the median values of each n-DGA and the benchmark, it is found that as n increases, the median of MSE decreases, indicating that n reduces the dissimilarity between the host and stego images. The same observation holds for PSNR and Correlation.

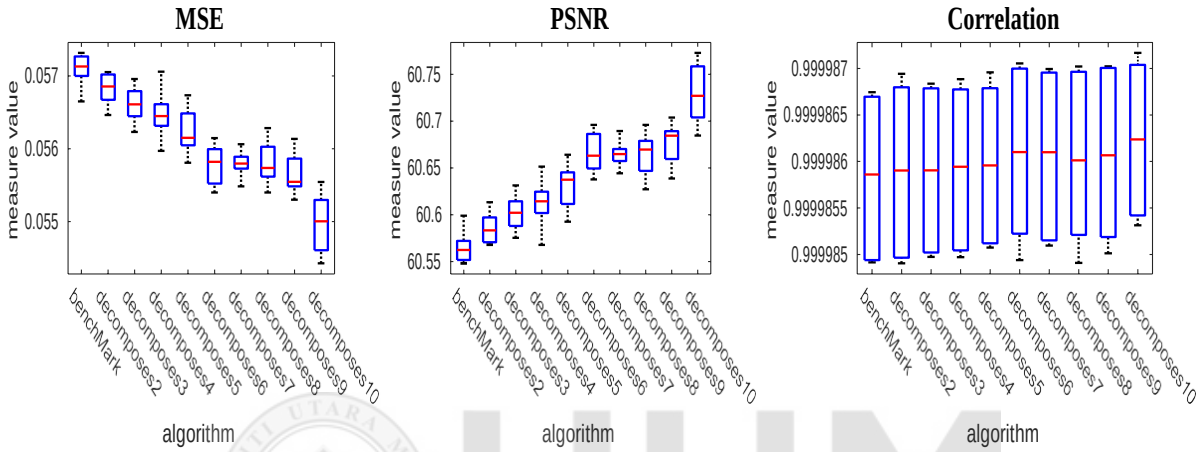


Figure 5.8 Imperceptibility evaluation metrics for n-DGA and its comparison with the benchmark for the Retina dataset

(iii) Brain Dataset

A set of Brain images were selected from a dataset provided by Kaggle using the URL https://www.kaggle.com/datasets/jakeshbohaju/Brain-tumor. These images are examples of common use in medical diagnosis; these images were used in the proposed technique for experimental purposes as a host to conceal the secret message. The Brain dataset provided numerical values for MSE, computed by Equation 3.3, as shown in Table 5.13. It is noted that the benchmark is superior to n-DGA, possibly because the Brain images are more homogeneous and have a wide black background.

Table 5.13

*MSE results for n-DGA a*nd comparison to the benchmark

Image No	Benchmark	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	0.0521	0.0534	0.0529	0.0547	0.0544	0.0550	0.0542	0.0550	0.0545	0.0536
2	0.0521	0.0515	0.0530	0.0541	0.0540	0.0533	0.0543	0.0550	0.0534	0.0531
3	0.0520	0.0516	0.0527	0.0547	0.0547	0.0544	0.0544	0.0551	0.0539	0.0530
4	0.0521	0.0516	0.0527	0.0541	0.0542	0.0529	0.0549	0.0549	0.0547	0.0537
5	0.0520	0.0533	0.0539	0.0548	0.0540	0.0532	0.0542	0.0544	0.0533	0.0530
6	0.0512	0.0538	0.0528	0.0539	0.0546	0.0541	0.0541	0.0550	0.0543	0.0530
7	0.0512	0.0511	0.0526	0.0536	0.0541	0.0529	0.0543	0.0553	0.0541	0.0528
8	0.0510	0.0524	0.0522	0.0544	0.0542	0.0529	0.0542	0.0551	0.0535	0.0533
9	0.0511	0.0528	0.0522	0.0553	0.0540	0.0528	0.0551	0.0548	0.0543	0.0545
10	0.0510	0.0511	0.0541	0.0538	0.0542	0.0541	0.0548	0.0546	0.0544	0.0533
Average	**0.0516**	**0.0523**	**0.0529**	**0.0543**	**0.0542**	**0.0535**	**0.0545**	**0.0549**	**0.0540**	**0.0533**

Based on the numerical results of the brain dataset, Figure 5.9 depicts a graphical representation of the MSE measurement of the brain dataset, in which the results of the proposed method are compared to the results of the benchmark method.

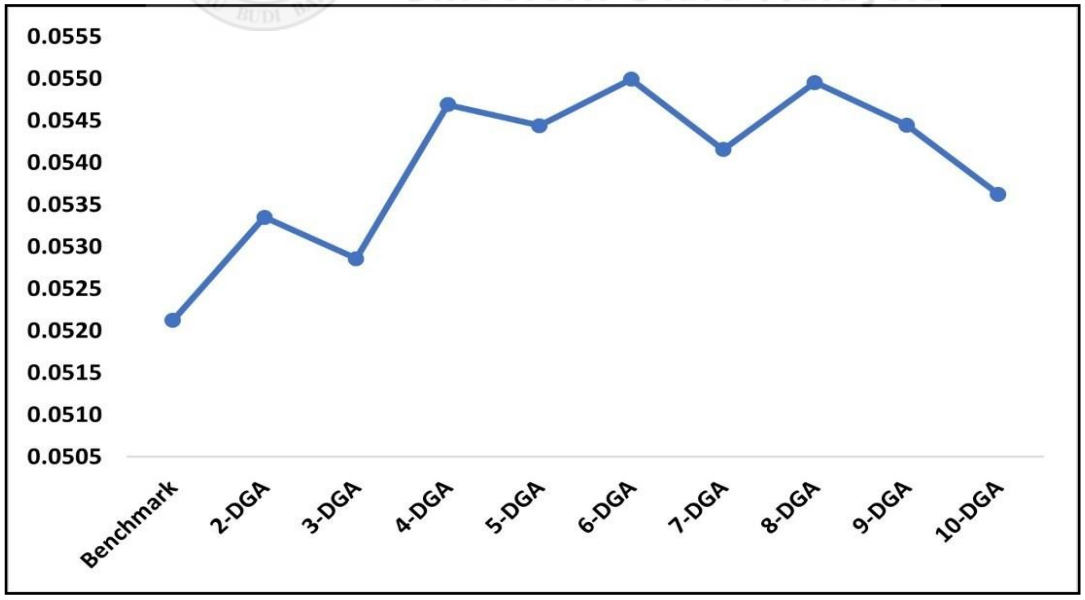


Figure 5.9 MSE Measure for Brain Dataset

Figure 5.9 revealed that the benchmark generated the lowest values In the MSE metric. In contrast, our developed DGA yielded greater values to MSE. Furthermore, we observe that an

increase in the value of n results in an increase in MSE. The MSE value when n = 10 is 0.0535, whereas the MSE value for the benchmark was between 0.0520 and 0.0525. This indicates that, unlike the two datasets (chest and retina), the developed method did not produce satisfactory outcomes. The homogeneity interprets this in the brain data compared with the other two datasets, which limits the decision of secret message insertion to a smaller region in the image. Consequently, dividing the image into blocks and enabling separate searching in each block causes sub-optimality.

The Brain dataset did not improve the MSE values for most of the images, as Table 5.14 shows a slight improvement in each image (2, 3, 4, and 7) when n equals two, i.e., 2-DGA, which are marked in bold.

Table 5.14

Improvement of the *MSE value* for the n-DGA *Brain* Dataset

Image-No	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	-0.0235	-0.0141	-0.0492	-0.0444	-0.0550	-0.0389	-0.0543	-0.0446	-0.0288
2	**0.0112**	-0.0170	-0.0392	-0.0366	-0.0228	-0.0429	-0.0550	-0.0260	-0.0194
3	**0.0069**	-0.0141	-0.0520	-0.0535	-0.0468	-0.0466	-0.0600	-0.0384	-0.0195
4	**0.0108**	-0.0106	-0.0371	-0.0393	-0.0143	-0.0522	-0.0533	-0.0501	-0.0302
5	-0.0253	-0.0361	-0.0534	-0.0386	-0.0216	-0.0425	-0.0460	-0.0235	-0.0179
6	-0.0496	-0.0310	-0.0513	-0.0650	-0.0557	-0.0558	-0.0733	-0.0601	-0.0343
7	**0.0033**	-0.0263	-0.0458	-0.0563	-0.0327	-0.0605	-0.0797	-0.0565	-0.0314
8	-0.0284	-0.0246	-0.0677	-0.0633	-0.0377	-0.0636	-0.0811	-0.0498	-0.0466
9	-0.0340	-0.0218	-0.0825	-0.0572	-0.0350	-0.0795	-0.0725	-0.0639	-0.0669
10	-0.0037	-0.0616	-0.0563	-0.0627	-0.0619	-0.0759	-0.0711	-0.0669	-0.0463

The PSNR values are presented numerically for the Brain dataset, similar to the Chest and Retina datasets, computed by Equation 3.4. As illustrated in Table 5.15, increasing n led to reducing the PSNR for n-DGA as the PSNR value for image one decreased to 60.8370 when n was equal to 10. Furthermore, despite the low value of n, the benchmark achieved a higher PSNR than the n-DGA. For instance, in image one, the PSNR value for the benchmark was

60.9601, while the value for 2-DGA was 60.8593. The PSNR measure of the brain dataset yielded the same observation as the MSE measure. Due to the homogeneity in the brain dataset, dividing the image into blocks and enabling separate searches in each block causes a sub-optimal solution.

Table 5.15

PSNR results for n-DGA and comparison to the benchmark

Image No	Benchmark	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	60.9601	60.8593	60.8995	60.7516	60.7714	60.7275	60.7942	60.7305	60.7707	60.8370
2	60.9630	61.0119	60.8898	60.7961	60.8068	60.8652	60.7805	60.7305	60.8515	60.8795
3	60.9748	61.0048	60.9140	60.7547	60.7486	60.7759	60.7771	60.7217	60.8111	60.8911
4	60.9598	61.0068	60.9140	60.8016	60.7924	60.8983	60.7386	60.7341	60.7474	60.8305
5	60.9684	60.8599	60.8145	60.7425	60.8037	60.8758	60.7878	60.7729	60.8673	60.8914
6	61.0354	60.8252	60.9026	60.8182	60.7619	60.8001	60.7994	60.7284	60.7820	60.8892
7	61.0364	61.0507	60.9237	60.8419	60.7985	60.8967	60.7811	60.7034	60.7976	60.9020
8	61.0588	60.9373	60.9534	60.7744	60.7921	60.8979	60.7909	60.7199	60.8478	60.8608
9	61.0503	60.9052	60.9566	60.7061	60.8086	60.9011	60.7181	60.7465	60.7814	60.7692
10	61.0588	61.0426	60.7991	60.8209	60.7945	60.7979	60.7410	60.7604	60.7774	60.8624
Average	**61.0066**	**60.9504**	**60.8967**	**60.7808**	**60.7879**	**60.8436**	**60.7709**	**60.7348**	**60.8034**	**60.8613**

To illustrate the results of the comparison between the proposed technique and the benchmark method of the PSNR, Figure 5.10 shows the graphical representation of the PSNR of the brain dataset.

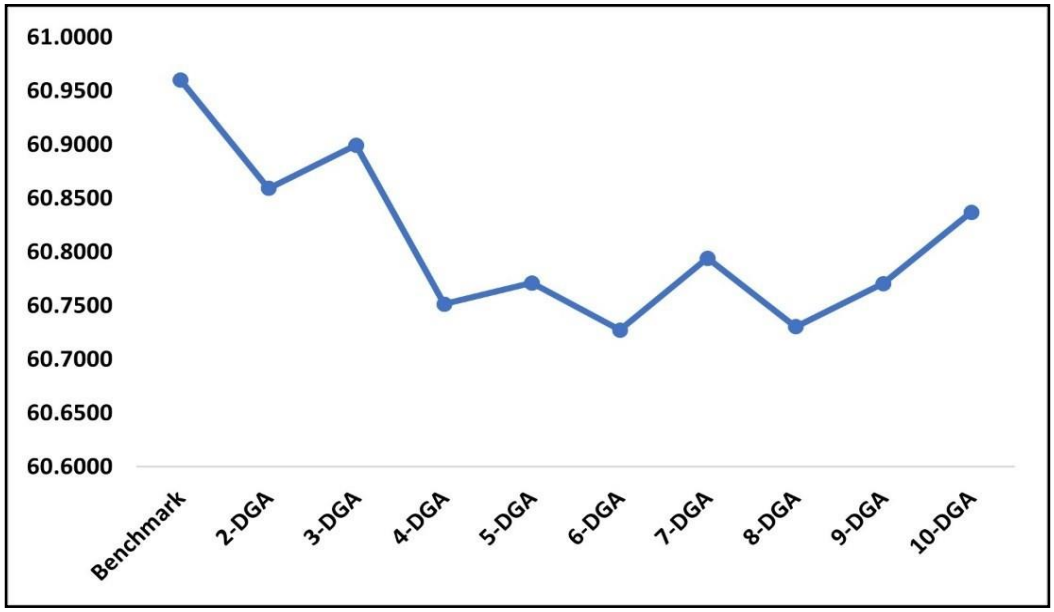


Figure 5.2 PSNR Measure for Brain Dataset

Similar to the MSE, the PSNR values of the benchmark recorded the highest values compared to those of the developed DGA method, as in Figure 5.10. In addition, an increase in the value of n led to a decrease in the PSNR values. Also, unlike the two datasets (chest and retina), the developed method did not yield satisfactory results.

Also, the Brain dataset did not enhance the PSNR values for most of the images, as Table 5.16 shows a slight improvement in each image (2, 3, 4, and 7) when n equals two, i.e., 2-DGA, which are marked in bold.

Table 5.16

Improvement of the PSNR value for the n-DGA Brain Dataset

Image-No	2-DGS	3-DGS	4-DGS	5-DGS	6-DGS	7-DGS	8-DGS	9-DGS	10-DGS
1	-0.0017	-0.0010	-0.0034	-0.0031	-0.0038	-0.0027	-0.0038	-0.0031	-0.0020
2	**0.0008**	-0.0012	-0.0027	-0.0026	-0.0016	-0.0030	-0.0038	-0.0018	-0.0014
3	**0.0005**	-0.0010	-0.0036	-0.0037	-0.0033	-0.0032	-0.0041	-0.0027	-0.0014
4	**0.0008**	-0.0008	-0.0026	-0.0027	-0.0010	-0.0036	-0.0037	-0.0035	-0.0021
5	-0.0018	-0.0025	-0.0037	-0.0027	-0.0015	-0.0030	-0.0032	-0.0017	-0.0013
6	-0.0034	-0.0022	-0.0036	-0.0045	-0.0039	-0.0039	-0.0050	-0.0042	-0.0024
7	0.0002	-0.0018	-0.0032	-0.0039	-0.0023	-0.0042	-0.0055	-0.0039	-0.0022
8	-0.0020	-0.0017	-0.0047	-0.0044	-0.0026	-0.0044	-0.0055	-0.0035	-0.0032
9	-0.0024	-0.0015	-0.0056	-0.0040	-0.0024	-0.0054	-0.0050	-0.0044	-0.0046
10	-0.0003	-0.0043	-0.0039	-0.0043	-0.0043	-0.0052	-0.0049	-0.0046	-0.0032

The correlation values are presented numerically for the Brain dataset, computed by Equation 3.5, similar to the Chest and Retina datasets. As illustrated in Table 5.17, increasing n reduced the correlation value for n-DGA as image one decreased to 0.999987988 when n was increased to 10. Furthermore, despite the low value of n, the benchmark achieved a higher correlation than the n-DGA. For instance, in image one, the correlation value for the benchmark was 0.999988389, while the value for 2-DGA was 0.999988172.

Table 5.17

*Correlation results for n-DGA a*nd comparison to the benchmark

Image No	Benchmark	2-DGA	3-DGA	4-DGA	5-DGA	6-DGA	7-DGA	8-DGA	9-DGA	10-DGA
1	**0.999988389**	0.999988172	0.999988122	0.99998821	0.999988355	0.999987564	0.99998777	0.999987574	0.999987976	0.999987988
2	0.999988327	**0.999988427**	0.999988041	0.999987787	0.999987771	0.999987995	0.999987753	0.999988163	0.999987865	0.99998792
3	0.999988338	**0.99998841**	0.999988157	0.999988243	0.999988396	0.999988348	0.999987728	0.999987968	0.999987833	0.99998822
4	0.999988316	**0.999988416**	0.999988156	0.999987834	0.999988395	0.999988114	0.999988147	0.99998793	0.999988041	0.999988043
5	0.999988325	0.999988195	0.999988244	0.999988212	**0.999988427**	0.999988013	0.999987815	0.999988294	0.999987932	0.999987982
6	**0.9999868**	0.999986012	0.999986188	0.999985879	0.999986451	0.999985816	0.999985959	0.999985619	0.999986151	0.999985998
7	**0.999986805**	0.999986702	0.999986374	0.999986113	0.999986448	0.999986192	0.999985826	0.999986017	0.999986343	0.999986079
8	**0.99998687**	0.999986379	0.999986517	0.99998578	0.999985883	0.999986208	0.999985831	0.999986226	0.999985968	0.999986421
9	**0.999986843**	0.999986214	0.999986525	0.999985713	0.999985851	0.999986241	0.999985948	0.999986351	0.999985948	0.99998603
10	**0.99998687**	0.999986687	0.999986327	0.999985892	0.999985902	0.999986618	0.999986554	0.99998569	0.999986511	0.999986482
Average	**0.999987588**	**0.999987361**	**0.999987265**	**0.999986966**	**0.999987188**	**0.999987111**	**0.999986933**	**0.999986983**	**0.999987057**	**0.999987116**

Figure 5.11 depicts a graphical representation of the correlation of the brain dataset and illustrates the results of a comparison between the proposed technique and the benchmark method.

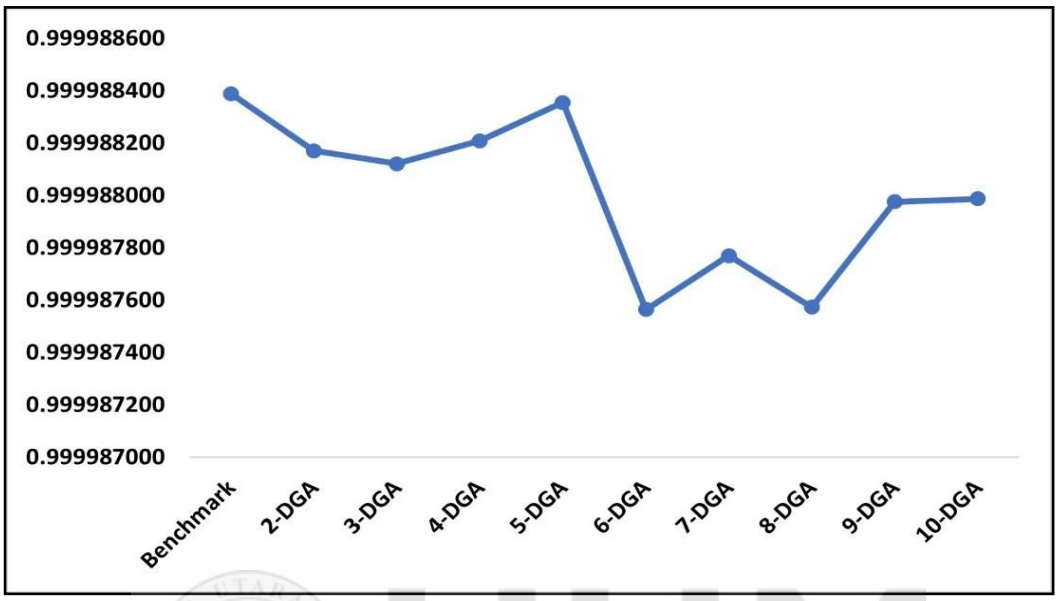


Figure 5.3 Correlation Measure for Brain Dataset

Also, the brain dataset did not achieve good results for the correlation measure. It is noted that the values of the correlation measure for the benchmark recorded the highest values compared to those of the DGA method developed as in Figure 5.11. In addition, an increase in the value of n led to a decrease in the correlation values. In addition, the correlation measure of the brain dataset yielded the same notices as the MSE and PSNR measures. Because brain images are homogeneous, dividing the image into blocks and enabling separate searches in each block results in a suboptimal solution.

Similar to MSE and PSNR, the improvement percentage in Correlation is presented in Table 5.18 for the Brain dataset. It is observed that there is a slight improvement in correlation values by increasing the value of n. For instance, 2-DGA for images (2, 3, and 4) and 5-DGA for images (3, 4, and 5). In comparison, the benchmark is superior in Correlation to the n-DGA in the remaining images.

Table 5.18

Improvement of the Correlation value for the n-DGA Brain Dataset

Image-No	2-DGA	3-DGA	4-DGA	5-DGA	6-DGA	7-DGA	8-DGA	9-DGA	10-DGA
1	-2.17562E-07	-2.676E-07	-1.79508E-07	-3.36622E-08	-8.24682E-07	-6.19042E-07	-8.15241E-07	-4.13048E-07	-4.01495E-07
2	**9.99767E-08**	-2.86148E-07	-5.3929E-07	-5.55455E-07	-3.31401E-07	-5.74155E-07	-1.63617E-07	-4.61983E-07	-4.06426E-07
3	**7.19157E-08**	-1.80685E-07	-9.45634E-08	**5.7956E-08**	1.0366E-08	-6.09848E-07	-3.699E-07	-5.05275E-07	-1.18052E-07
4	**1.00112E-07**	-1.59837E-07	-4.81801E-07	**7.89461E-08**	-2.01906E-07	-1.69486E-07	-3.86535E-07	-2.75082E-07	-2.72682E-07
5	-1.30142E-07	-8.15592E-08	-1.13294E-07	**1.02049E-07**	-3.12007E-07	-5.09984E-07	-3.19197E-08	-3.93576E-07	-3.43731E-07
6	-7.87515E-07	-6.11806E-07	-9.20641E-07	-3.48748E-07	-9.83788E-07	-8.40465E-07	-1.18103E-06	-6.49217E-07	-8.0207E-07
7	-1.02963E-07	-4.30512E-07	-6.91357E-07	-3.57037E-07	-6.12096E-07	-9.78547E-07	-7.8719E-07	-4.61837E-07	-7.25105E-07
8	-4.90706E-07	-3.53011E-07	-1.08982E-06	-9.86811E-07	-6.61751E-07	-1.03846E-06	-6.44135E-07	-9.02262E-07	-4.49166E-07
9	-6.28119E-07	-3.1793E-07	-1.12972E-06	-9.91437E-07	-6.01854E-07	-8.94508E-07	-4.91245E-07	-8.95016E-07	-8.1275E-07
10	-1.8337E-07	-5.43056E-07	-9.78039E-07	-9.67706E-07	-2.5191E-07	-3.16328E-07	-1.18014E-06	-3.58787E-07	-3.87434E-07

Comparing the median values of each n-DGA and the benchmark shows that as n increases, the median of MSE increases. A possible reason is that Brain images are more homogeneous and have an extensive black background, so the distribution of the message may damage the image by embedding the secret bits in the background. The same conclusion holds for PSNR and Correlation. As illustrated in Figure 5.12, the benchmark's metrics MSE, PSNR, and Correlation outperformed all n-DGA configurations.

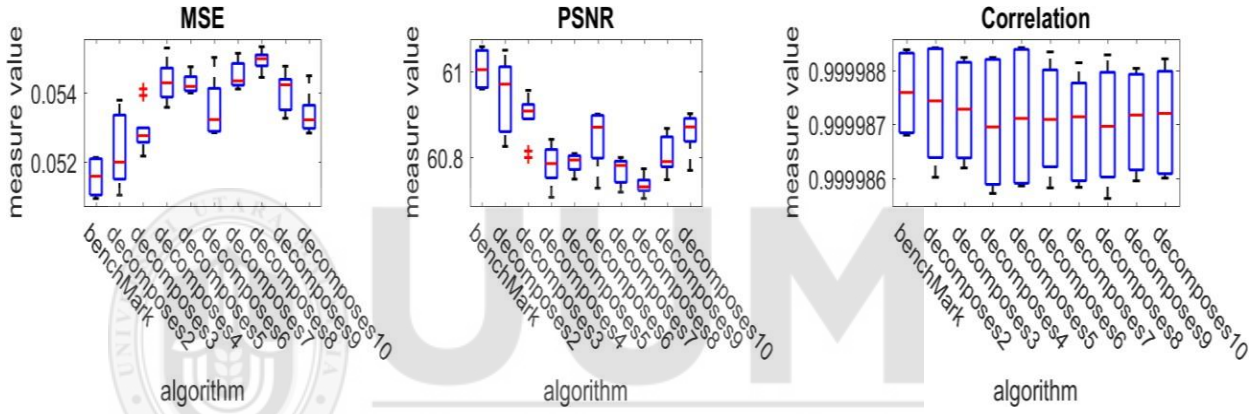


Figure 5.4 Imperceptibility evaluation metrics for n-DGA and its comparison with the benchmark for the Brain dataset

5.2.2 Security

The second challenging feature of steganography is the inability of intruders to discover the message statistically. The steganography system is successful if the attacker cannot detect the hidden sensitive or significant information. Technically, steganalysis aims to test the strength of the steganography system by detecting the presence of secret messages. Typically, analysts use two types of analysis, passive and active. Passive steganalysis is not concerned with preserving the payload because its goal is to corrupt and distort the confidential information contained in the host, thus destroying the purpose of the safe

transmission of hidden messages. Active steganalysis works to extract the payload instead of destroying it by discovering the exact algorithm used to hide messages. This research presents Regular-Singular (RS) analysis and histogram as security metrics to measure statistical steganalysis between the host image and stego-image. RS and histogram are the most effective analysis methods for steganography techniques to determine whether an image contains a hidden message by analyzing the double-statistics of host and stego images.

The first evaluation is that the RS analysis exploits the Correlation in the spatial domain to estimate the message hidden in the host image, where the LSB method was used to hide the message. The fact of RS analysis is that it depends on the content of each bit level in the image related to the other bit levels, i.e., analyzing how the number of R and S groups of pixels changes with the increase in the length of the embedded message in the LSB level.

Figures 5.13 (a), (b), and (c) depict the RS analysis evaluation for the benchmark and the developed n-DGA algorithms for Chest, Retina, and Brain datasets, respectively. The X-axis represents the percentage of hiding capacity, and the Y-axis represents the percentage of regular (R) or singular (S) groups.

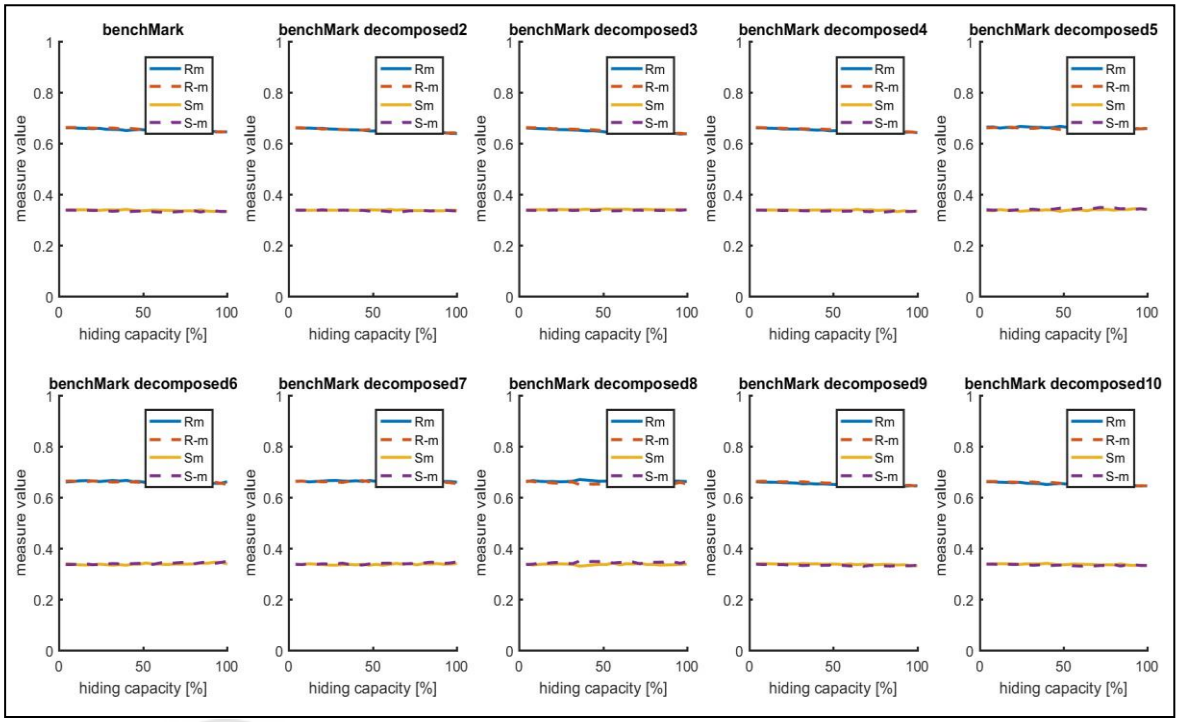


Figure 5. 5 (a) RS analysis for n-DGA and Its Comparison with the Benchmark for the Chest Dataset

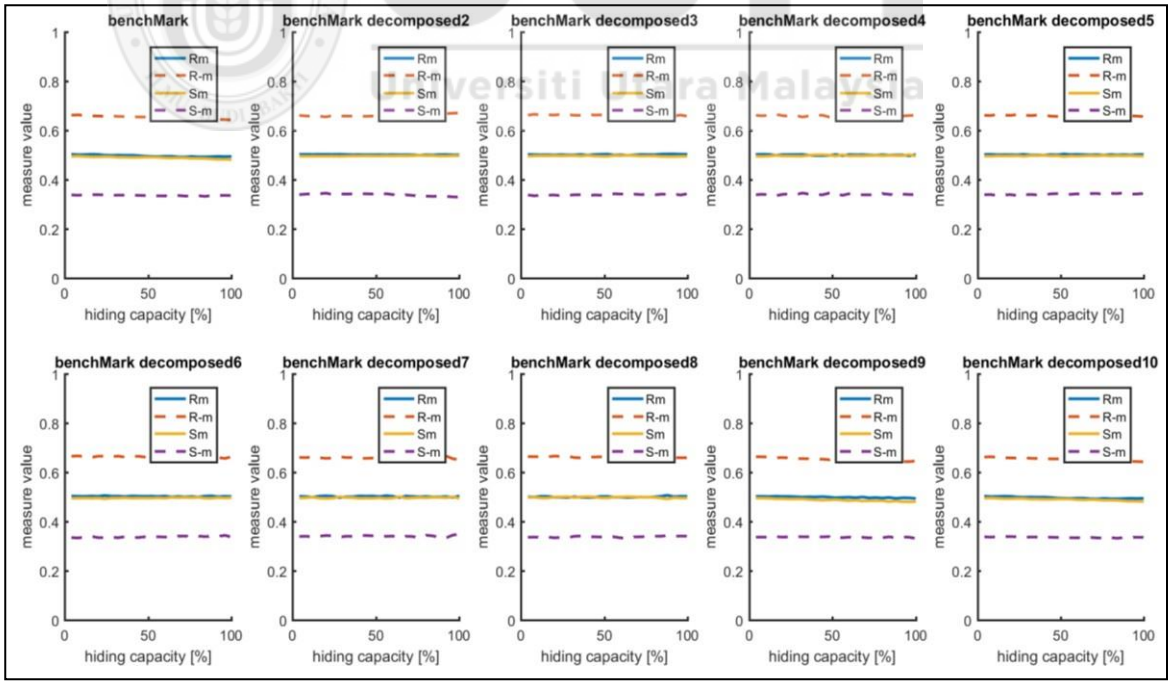


Figure 5. 6 (b) RS analysis for n-DGA and Its Comparison with the Benchmark for the Retina Dataset

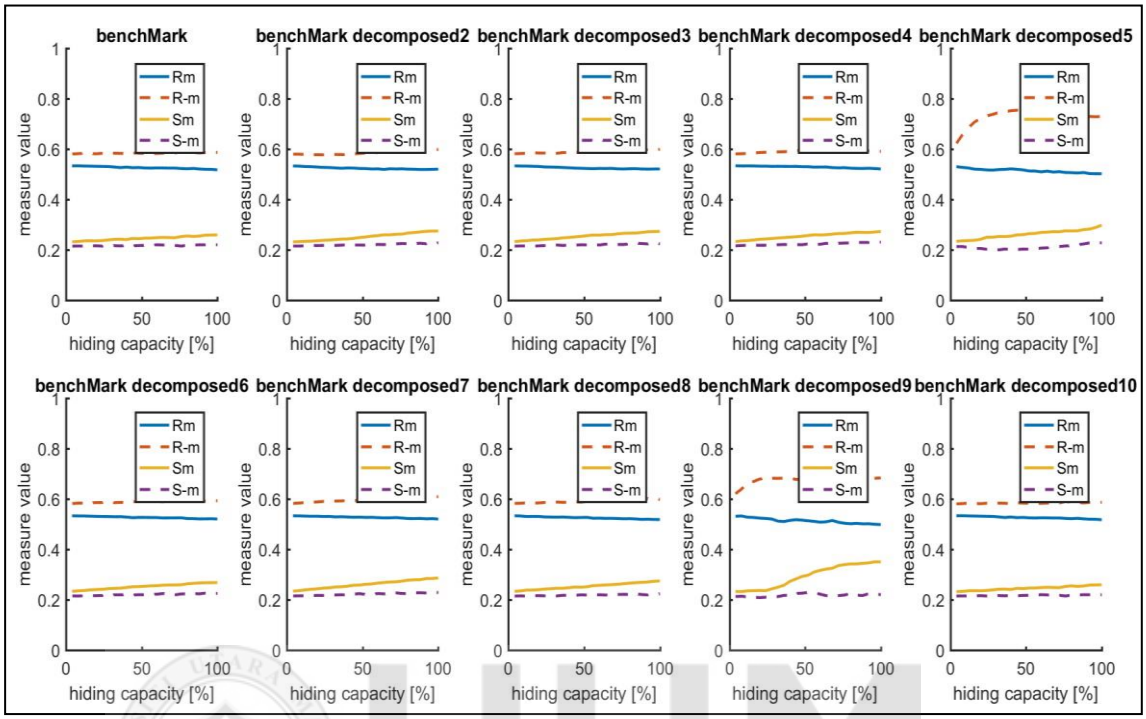


Figure 5. 13 (c) RS analysis for n-DGA and Its Comparison with the Benchmark for the Brain Dataset

As can be seen from Figures 5.13 (a) and (b), it is found that the difference between the ratios R_m and S_m of the stego-image is low, while the difference between the ratios R_{-m} and S_{-m} is increasing, that is, R_{-m}- S_{-m} > R_m- S_m. Hence, all methods are secure against RS analysis for Chest and Retina datasets. While the benchmark of the Brain dataset outperformed most of the n-DGA techniques, as shown in Figure 5.13 (c).

The second evaluation is the histogram showing the concealed message's presence, where it visualizes the differences between the host image and the stego-image based on the methods developed. The benchmark has been observed to most deviate from the host image for both Chest and Retina datasets, as shown in Figures 5.14 (a) and (b), respectively. At the same time, all n-DGA methods produced graph values closer to the

host image, implying more steganographic quality. While the benchmark of the Brain dataset outperformed some of the n-DGA techniques, as shown in Figure 5.14 (c).

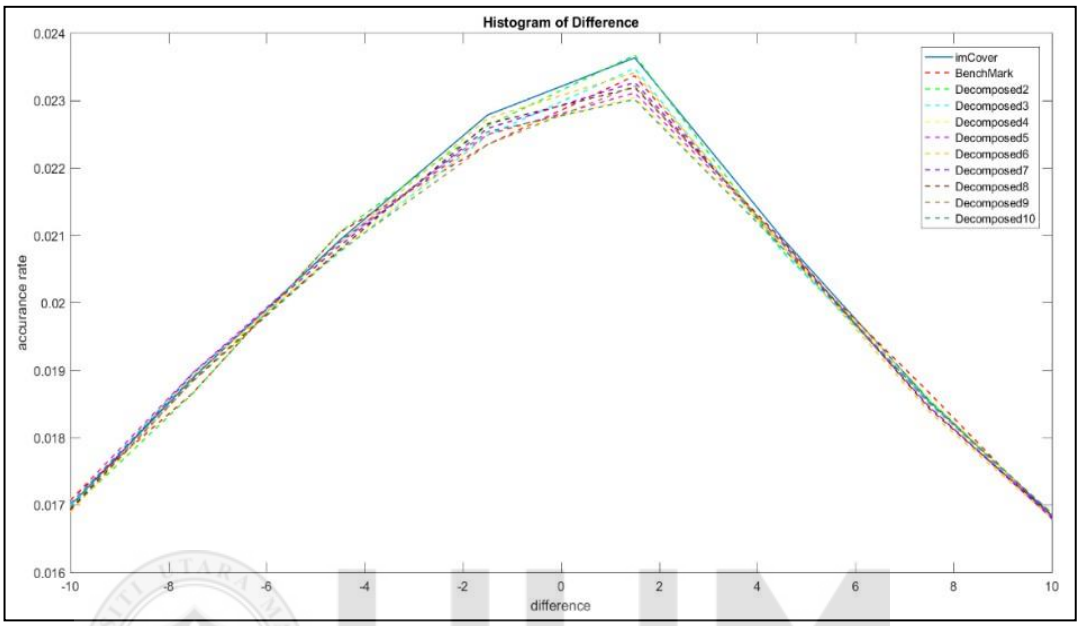


Figure 5.14 (a) Histogram Evaluation for n-DGA and Its Comparison with the Benchmark for the Chest Dataset

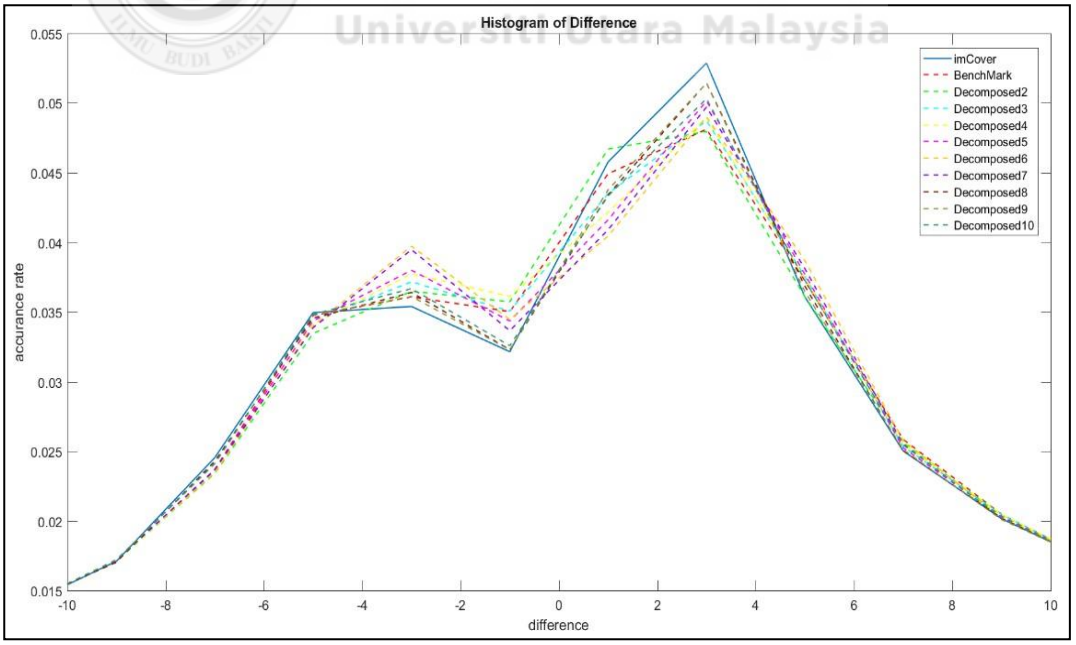


Figure 5.14 (b) Histogram Evaluation for n-DGA and Its Comparison with the Benchmark for the Retina Dataset

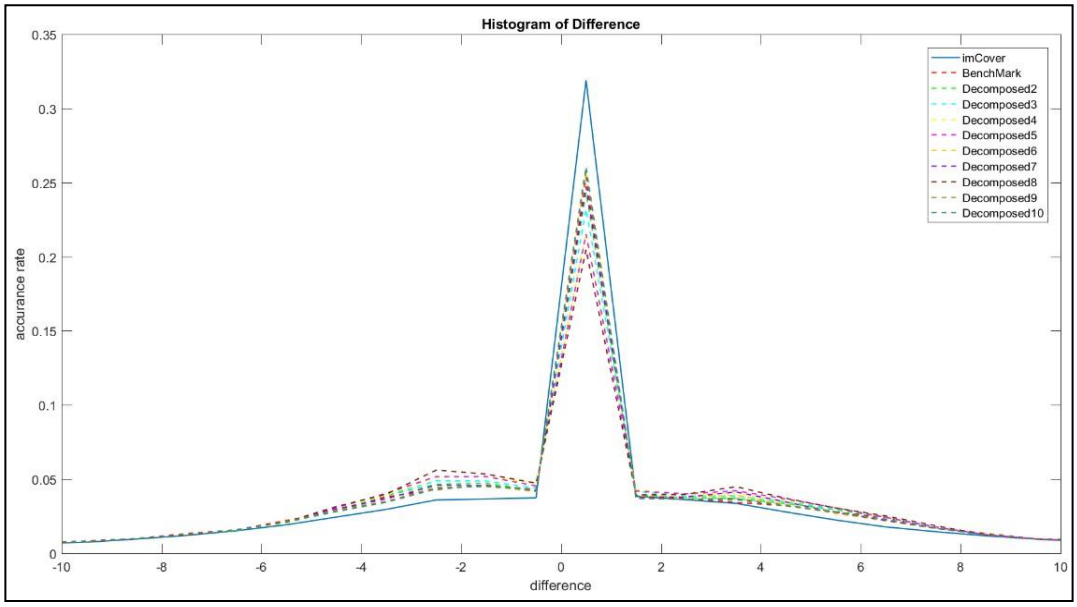


Figure 5. 14 (c) Histogram Evaluation for n-DGA and Its Comparison with the Benchmark for the Brain Dataset

To display the histogram analysis result. One image was taken from each Chest, Retina, and Brain dataset. Tables 5.19, 5.20, and 5.21 compare histogram analysis for the original images and the stego-images generated from the benchmark and n-DGA proposed algorithm. When the secret message bits are embedded in the host image, the frequency of pixel values changes and may become obvious (attracting attention) in the histogram.

Table 5.19

Comparison of the Chest image histogram analysis for the n-DGA and the benchmark algorithms

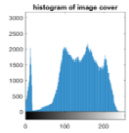
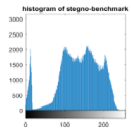
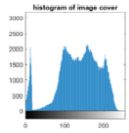
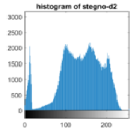
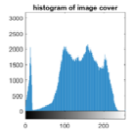
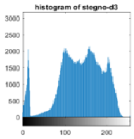
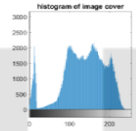
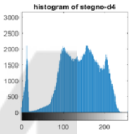
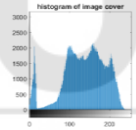
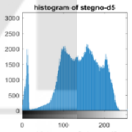
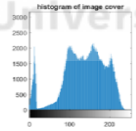
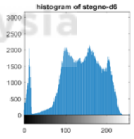
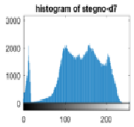
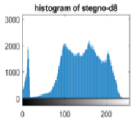
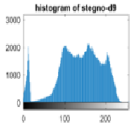
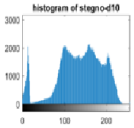
Algorithms	Host-Image	Histogram	Stego-Image	Histogram
Benchmark				
2-DGA				
3-DGA				
4-DGA				
5-DGA				
6-DGA				
7-DGA				
8-DGA				
9-DGA				
10-DGA				

Table 5.20

Comparison of the Retina image histogram analysis for the n-DGA and the benchmark algorithms

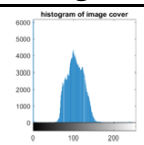
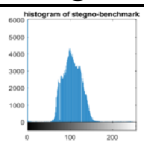
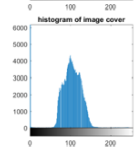
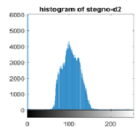
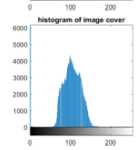
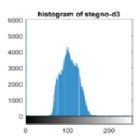
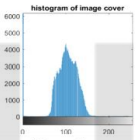
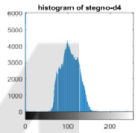
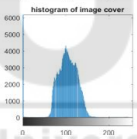
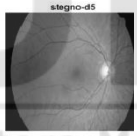
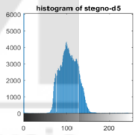
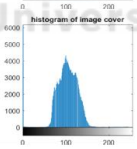
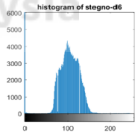
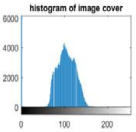
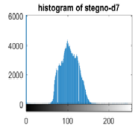
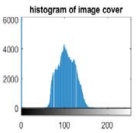
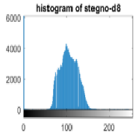
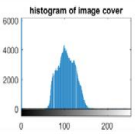
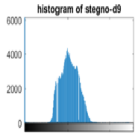
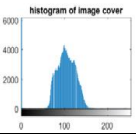
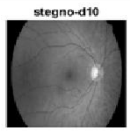
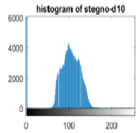
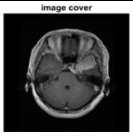
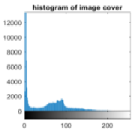
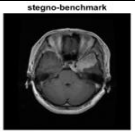
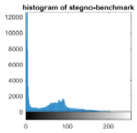
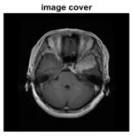
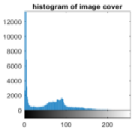
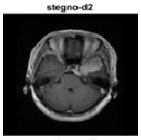
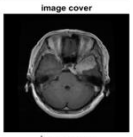
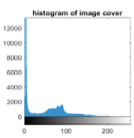
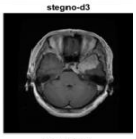
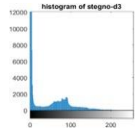
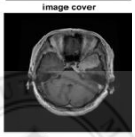
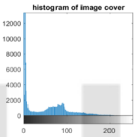
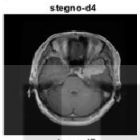
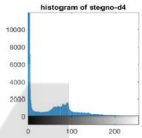
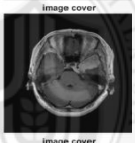
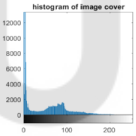
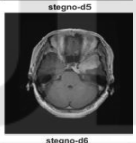
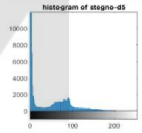
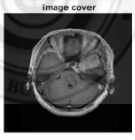
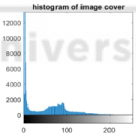
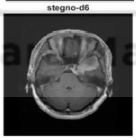
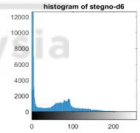
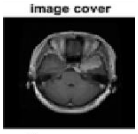
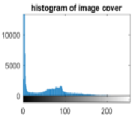
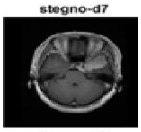
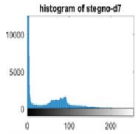
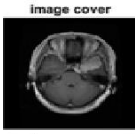
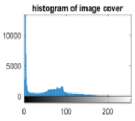
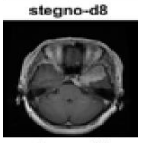
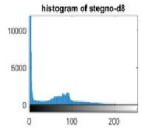
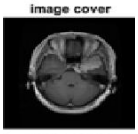
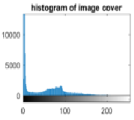
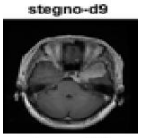
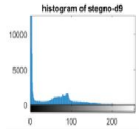
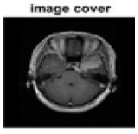
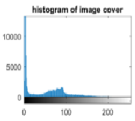
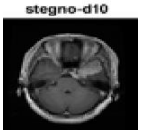
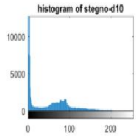
Algorithms	Host-Image	Histogram	Stego-Image	Histogram
Benchmark				
2-DGA				
3-DGA				
4-DGA				
5-DGA				
6-DGA				
7-DGA				
8-DGA				
9-DGA				
10-DGA				

Table 5.21

Comparison of the Brain image histogram analysis for the n-DGA and the benchmark algorithms

Algorithms	Host-Image	Histogram	Stego-Image	Histogram
Benchmark				
2-DGA				
3-DGA				
4-DGA				
5-DGA				
6-DGA				
7-DGA				
8-DGA				
9-DGA				
10-DGA				

According to the analysis results, the histograms of the host and stego-images showed no discernible difference. As histogram analysis indicates, the variation between the produced histograms is comparatively decreased for all examined images. The embedded data is difficult to discover using difference histogram analysis. As a result, the proposed technique is immune to steganalysis attacks based on histograms. The confidential data's security was secured while maintaining the proposed method's high visual quality.

5.3 Discussion

The proposed medical image steganography scheme has addressed important issues: imperceptibility (reducing distortion from embedding secrets) and security (preventing statistical detection of the difference between the host image and the resulting stego-image). Our developed n-DGA differs from the benchmark in two aspects: embedding the secret message in n-DGA is enabled in various non-connected regions, whereas the benchmark embeds the secret message in the connected region. Therefore, the security of n-DGA is greater than that of the benchmark. In addition, the imperceptibility is increased by dispersing the secret message throughout the image.

Hiding secret information in the host image has changed some basic image information, so it is necessary to ensure that the proposed scheme that affected image quality is addressed after embedding. The evaluation of the proposed scheme relied on objective methods to find the difference and similarity between the two host and stego images through numerical criteria, including MSE, PSNR, and Correlation, and statistical methods, such as histogram and RS.

Through the numerical results of three datasets: chest, retina, and brain, which are used to compare the proposed scheme with the benchmark, Tables 5.1 and 5.7 clearly show that all n values are superior in terms of MSE compared to the benchmark for the Chest and Retina datasets. The higher the value of n, the greater the degree of imperceptibility that a lower value of MSE provides. As a result, it was concluded that n-DGA is superior to the benchmark. Moreover, it also concluded that n is a performance control parameter. In addition, the Chest dataset achieved the lowest value for the MSE metric, 0.0557, while the benchmark achieved 0.0582. It was followed by the Retina dataset, which had the lowest MSE value of 0.0550, while the benchmark achieved 0.0571. At the same time, Table 5.13 shows the superiority of the benchmark over the proposed method for the Brain dataset; increasing the value of n did not decrease the value of MSE.

Also, Tables 5.3 and 5.9 clearly show that all n values are superior in terms of PSNR compared to the benchmark for the Chest and Retina datasets. The higher value of n, the greater the degree of imperceptibility that a higher value of PSNR provides. As a result, it was concluded that n-DGA is superior to the benchmark. Furthermore, it also concluded that n is a parameter controlling the performances. In addition, the Chest dataset came out with the highest value of the PSNR metric, 60.6696, while the benchmark achieved 60.4829. It was followed by the Retina dataset, which achieved the highest value of the PSNR, 60.7287, while the benchmark achieved 60.5647. While Table 5.15 shows the superiority of the benchmark over the proposed method for the Brain dataset, the increase of the n value did not increase the PSNR value.

Similar to MSE and PSNR metrics, Tables 5.5 and 5.11 clearly show that all n values are superior in Correlation (r) compared to the Chest and Retina datasets benchmark. The

higher value of n, the greater the degree of imperceptibility that a higher value of (r) provides. As a result, it was concluded that n-DGA is superior to the benchmark. Furthermore, it also concluded that n is a parameter controlling the performance. Likewise, the correlation metric achieved the highest value for the Chest dataset among the datasets, as it achieved 0.99999014, while the benchmark achieved 0.999989711. The Retina dataset followed by achieving the highest 0.999986234, while the benchmark achieved 0.999985829. While the Brain dataset, as in Table 5.17, shows that the increase of the n value did not increase the correlation value, just a slight improvement.

5.4. Summary

The chapter starts with the experimental results and analysis, where the evaluation was conducted on three datasets: Chest, Retina, and Brain. The most common performance metrics used in this chapter's evaluation: are MSE, PSNR, Correlation (r), histogram, and RS. In addition, the statistical analysis and numerical results are presented. The analysis has shown that increasing the value of n implies improving the imperceptibility and security performance.

Furthermore, it is found that despite the value of n, there was always superiority of n-DGA over the benchmark. In addition, it is observed that increasing the value of n implies more divisions, which consequently leads to more computational cost. Hence, n is the controlling parameter for the trade-off between efficiency and effectiveness.

CHAPTER SIX
CONCLUSIONS AND FUTURE WORK

6.1 Introduction

This chapter elaborates on the summary of this research, accompanied by future work for intended interested researchers. It is decomposed into five sections—Section 6.2 reports revisiting the research objectives. Next, the research results summary is presented in Section 6.3, detailed in the previous chapter. Contributions were presented in Section 6.4. Afterward, Section 6.5 lists the limitations of this research. This chapter ends with future works and recommendations Section in section 6.6.

6.2 Revisiting Research Objectives

Steganography is an active security topic that involves hiding data in reliable mediums. The medium might be an image or audio file used as a host. The hiding is regarded as an NP-hard optimization problem. It optimizes a formulated objective function that indicates the image's imperceptibility. Indeed, most current proposed methods in the literature considering imperceptibility and security continue to suffer from various issues. One of the common approaches for handling steganography is random searching using meta-heuristic searching algorithms.

This research achieved four objectives in concealing medical images, each of which was achieved as follows: the first objective until the third objective in Chapter 4, and the fourth objective in Chapter 5. This section is divided into subsections: Subsection 6.2.1 deals with the first objective. Subsection 6.2.2 achieves the second objective. The third objective is presented in subsection 6.2.3. Finally, subsection 6.2.4 lists the stage of evaluation of the proposed system.

6.2.1 Objective 1: Formulation of an Embedding Scheme for Avoiding the Non-Valid Implicit Constraints

The message length and the high number of possibilities for inserting the message inside the image causes a huge number of possibilities and degradation in the convergence performance toward the optimal insertion. To handle a huge number of possibilities and degradation in the convergence, the first objective has focused on formulating an embedding scheme to avoid the non-valid implicit constraints contributing to reducing the solution space. In this formulation, the embedding of the message within the image is not supposed to be in a continuous region nor in any direction to ensure the integrity of the diagnosis's important region.

6.2.2 Objective 2: Propose a Decomposition Controlling Parameter Scheme to Cater Lack of Convergence and Address the Application's Customizability

In addition, as a second objective, for this purpose, n-Decomposition Genetic-based steganography (n-DGA) is proposed, representing a novel approach for steganography to increase imperceptibility and security so that the intruders or unauthorized would be unable to recognize them. The increase in imperceptibility is enabled by improving the convergence of the optimization based on more than one optimization conducted on reduced solution space. The increase in security is enabled by improving the selection of the inserted regions from connected to non-connected areas. The n-DGA algorithm decomposes the message into parts, enabling a standalone optimization for each part. This optimization provides dysconnectivity in the message over the image and leads to more security. The n-DGA algorithm provides a variable-length searching, making it distinguishable from other optimization algorithms in violating the implicit constraint that

causes local minima trap and affects security. In the resulting technique, the user determines the decomposition value, an integer that balances security and imperceptibility based on the user's preferences.

6.2.3 Objective 3: Integrate the Two Proposed Schemes into a Single Technique

As a third objective, the formulation in objective one has been integrated with the algorithm of n-DGA decomposition in the second objective to provide one technique for steganography. This algorithm enables embedding a secret message into the medical image with controlling desired imperceptibility and security.

6.2.4 Objective 4: Evaluate the Proposed Technique Using Standard Evaluation Metrics and Compare It with Suitable Benchmark Studies

As previously stated, every steganography system is susceptible to various attacks. The secret message bits are concealed within an image to ensure the secure transmission of data and prevent attacks. Over the years, numerous methods have been developed, mostly based on the LSB embedding technique. However, few new techniques have been developed to defend against common attacks. According to this factor, the proposed scheme protected the system against attacks and concealed the secret message from unauthorized parties. As a fourth objective, a thorough evaluation of n-DGA has shown its superiority over classical whole message optimization in all imperceptibility and security measures. The evaluation has shown that the n-DGA has accomplished higher values of PSNR compared with the benchmark and fewer values of MSE.

6.3 Research Results Summary

The research has presented several findings. They can be stated as follows.

(1) The research has shown that steganography based on inserting the message in scattered locations in the host image is superior that steganography based on inserting the message in connected locations.

(2) The research provided that increasing the number of parts when decomposing the message into parts helps increase imperceptibility. However, it leads to more computational load due to calling more than one genetic optimization. Hence, it is important to control effectiveness vs. efficiency using external controlling parameters.

(3) The research has shown that decomposing the message into parts and embedding them in separate places helps to avoid embedding confidential information on top of critical diagnostic information to rule out damage. Hence, this research increases the algorithm's applicability in the medical domain.

6.4 Contributions

This research aims to develop a robust medical image steganography scheme capable of withstanding multiple attacks, thus enhancing its security with a high grade of imperceptibility. Security and imperceptibility are key requirements for any steganography system (Thabit, 2021; Kadhim et al., 2019). As a result, in this research, their contributions to the steganography area were carefully considered.

The theoretical contributions can be summarized as follows:

(1) To our knowledge, this is the first genetic-based steganography to insert the secret message into scattered regions in the host image with different embedding configurations in each region.

(2) This research proposed a novel concept designated as Genetic based decomposition. The increased degree of freedom in the developed steganography provides more security. It does not conflict with efficiency and convergence, considering that genetics is applied more than once with a reduced set of solution spaces.

(3) As another theoretical contribution, it provides novel chromosome representation for steganography that enables controlling not only embedding the secret message in different positions, directions, bits, and polarization.

As for the practical contributions to this research, they can be mentioned below:

(1) It enables steganography's performance interactively using the controlling parameter n, which provides a trade-off between effectiveness and efficiency.

(2) The developed algorithm was evaluated using more than one type of medical image, and a display of the embedding locations of the secret message was provided alongside the performance metrics.

6.5 Limitations of the work

Several limitations can be associated with this work and can be presented as follows:

(1) The computational cost increases with increasing the value of n. Hence, a trade-off between efficiency and effectiveness is required. So, future work will investigate the value of n suitable for a certain type of application.

(2) The number of divisions might not be optimal to meet certain performance requirements. Searching for the optimal value of n can be incorporated into optimization or searching algorithms in future work to select the suitable algorithm for this optimization for handling this limitation.

6.6 Future Works and Recommendations

Several future works can be associated with this work and can be presented as follows:

(1) Moving from a meta-heuristic-based method to a reinforcement learning-based method with the same message decomposition concept. The benefit of the reinforcement learning-based method is building an entity or learned agent that captures the knowledge instead of relying only on current candidate solutions inside the population. Hence, the usage of reinforcement learning should enhance the convergence compared with the meta-heuristic.

(2) Extending the same approach to operate on different signals or mediums, such as voice and image hiding inside the host image. This is demanded from an application perspective due to the spread of multi-media-based applications.

(3) Converting the current optimization from one objective to multiple objectives enables setting a decision point inside the Pareto front to meet certain application requirements. As a result, interacting with the user to accept their preference is more feasible than the single optimization approach. Furthermore, multi-objective optimization provides the capability of escaping from local minima traps.

REFERENCE

Abdel-Basset, M., Abdel-Fatah, L., & Sangaiah, A. K. (2018). Metaheuristic algorithms: A comprehensive review. Computational intelligence for multimedia big data on the cloud with engineering applications, 185-231.

Abdulateef, S. K., Ahmed, S. R. A., & Salman, M. D. (2020, November). A Novel Food Image Segmentation Based on Homogeneity Test of K-Means Clustering. In IOP Conference Series: Materials Science and Engineering (Vol. 928, No. 3, p. 032059). IOP Publishing.

Abdulateef, S. K., Mahmuddin, M., & Harun, N. H. (2017). Food image representation based on modified orientation map. Journal of Theoretical and Applied Information Technology, 95(1), 40-46.

Abdullah, A. saadi, & Hussein, Q. M. (2020). Using Digital Image as a Cover of Information Hiding: Review Paper. IOP Conference Series: Materials Science and Engineering, 928(3). https://doi.org/10.1088/1757-899X/928/3/032085.

Abdulwahed, M. N. (2019). Digital image steganography scheme based on SK-LSB substitution and three parameters encryption method. Journal of Theoretical and Applied Information Technology, 97(15), 4116–4137.

Abood, Z. M. (2013). Edges enhancement of medical color images using add images. IOSR Journal of Research & Method in Education, 2(4), 52-60.

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1), 1-18.

AbuTaha, M., Farajallah, M., Tahboub, R., & Odeh, M. (2011). Survey paper: cryptography is the science of information security.

Agarwal, P., & Mehta, S. (2018). Empirical analysis of five nature-inspired algorithms on real parameter optimization problems. Artificial Intelligence Review, 50(3), 383-439.

Agrawal, P., Abutarboush, H. F., Ganesh, T., & Mohamed, A. W. (2021). Metaheuristic Algorithms on Feature Selection: A Survey of One Decade of Research (2009-2019). IEEE Access, 9, 26766-26791.

Ahmad, T., Studiawan, H., Ahmad, H. S., Ijtihadie, R. M., & Wibisono, W. (2014). Shared secret-based steganography for protecting medical data. In 2014 International Conference on Computer, Control, Informatics and Its Applications (IC3INA) (pp. 87-92). IEEE.

Ahuja, B., & Kaur, M. (2009). High capacity filter based steganography. International Journal of Recent Trends in Engineering, 1(1), 672.

Akhtar, N. (2016). An Efficient Lossless Modulus Function Based Data Hiding Method. In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics (pp. 281-287). Springer, New Delhi.

Al-Afandy, K. A., Faragallah, O. S., ELmhalawy, A., El-Rabaie, E. S. M., & El-Banby, G. M. (2016). High security data hiding using image cropping and LSB least significant bit steganography. In 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt) (pp. 400-404). IEEE.

Albadr, M. A., Tiun, S., Ayob, M., & AL-Dhief, F. (2020). Genetic Algorithm Based on Natural Selection Theory for Optimization Problems. Symmetry, 12(11), 1758.

Al-Dmour, H. S. T. (2018). Enhancing information hiding and segmentation for medical images using novel steganography and clustering fusion techniques (Doctoral dissertation).

Al-Dmour, H., & Al-Ani, A. (2015). Quality optimized medical image steganography based on edge detection and hamming code. In 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI) (pp. 1486-1489). IEEE.

Al-Dmour, H., & Al-Ani, A. (2016). Quality optimized medical image information hiding algorithm that employs edge detection and data coding. Computer methods and programs in biomedicine, 127, 24-43.

Al-Haj, A. (2015). Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. Journal of digital imaging, 28(2), 179-187.

Al-Khafaji, G., Taher, H. B., & Abdulzahara, N. A. (2014). Increase the Capacity Amount of Data Hiding to Least Significant BIT Method.

Almazaydeh, W. E. I. A. & Sheshadri, H. S. (2018). Image Steganography Using a Dynamic Symmetric Key. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1507-1513). IEEE.

Al-Mohammad, A. (2010). Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility (Doctoral dissertation, Brunel University, School of Information Systems, Computing and Mathematics Theses).

Almohammad, A., & Ghinea, G. (2010). Stego image quality and the reliability of PSNR. In 2010 2nd International Conference on Image Processing Theory, Tools and Applications (pp. 215-220). IEEE.

Almutairi, A. (2018). A Comparative Study on Steganography Digital Images: A Case Study of Scalable Vector Graphics (SVG) and Portable Network Graphics (PNG) Images Formats. Int. J. Adv. Comput. Sci. Appl, 9, 170-175.

Alobaedy, M. M. T. (2015). Hybrid ant colony system algorithm for static and dynamic job scheduling in grid computing (Doctoral dissertation, PhD Thesis, Universiti Utara Malaysia).

Al-Rababah, M., & Al-Marghirani, A. (2016). Implementation of novel medical image compression using artificial intelligence. Int. J. Adv. Comput. Sci. Appl, 7(5), 328-332.

Al-Saedi, A. K. H. (2016). A method to hide text in image. Journal of Misan Researches, 12(24), 11-23.

Al-Ta'i, Z. T. M., Abass, J. M., & Abd Al-Hameed, O. Y. (2017). Image steganography between Firefly and PSO Algorithms. International Journal of Computer Science and Information Security, 15(2), 9.

Al-Tamimi, A. G. T., & Alqobaty, A. A. (2015). Image steganography using least significant bits (LSBs): a novel algorithm. International Journal of Computer Science and Information Security, 13(1), 1.

Amirtharajan, R., Akila, R., & Deepikachowdavarapu, P. (2010). A comparative analysis of image steganography. International journal of computer applications, 2(3), 41-47.

Amirtharajan, R., Subrahmanyam, R., Prabhakar, P. J., Kavitha, R., & Rayappan, J. B. B. (2011, December). MSB over hides LSB—A dark communication with integrity. In 2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application (pp. 1-6). IEEE.

Anandpara, D., & Kothari, A. (2015). Working and comparative analysis of various spatial based image steganography techniques. International Journal of Computer Applications, 113(12).

Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2019). A comparative study of recent steganography techniques for multiple image formats. International Journal of Computer Network and Information Security, 11(1), 11.

Aparna, P., & Kishore, P. V. V. (2018). An efficient medical image watermarking technique in E-healthcare application using hybridization of compression and cryptography algorithm. Journal of Intelligent Systems, 27(1), 115-133.

Arif, A. S. (2015). Lossless and near lossless compression of pharynx and esophagus in fluoroscopy medical images (Doctoral dissertation, Multimedia University (Malaysia)).

Arumugham, S., Rajagopalan, S., Rayappan, J. B. B., & Amirtharajan, R. (2018). Networked medical data sharing on secure medium–A web publishing mode for DICOM viewer with three layer authentication. Journal of biomedical informatics, 86, 90-105.

Arunkumar, S., Subramaniyaswamy, V., & Sivaramakrishnan, N. (2018). Reversible data hiding scheme using modified histogram shifting in encrypted images for bio-medical images. International Journal of Pure and Applied Mathematics, 119(12e), 13233-13240.

Arunkumar, S., Subramaniyaswamy, V., Vijayakumar, V., Chilamkurti, N., & Logesh, R. (2019). SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. Measurement, 139, 426-437.

Astuti, W., & Wisety, U. N. (2015). Data Hiding Scheme on Medical Image using Graph Coloring. In Journal of Physics: Conference Series (Vol. 622, No. 1, p. 012028). IOP Publishing.

Atawneh, S. H. S. (2015). Enhanced Algorithms for Secure and Imperceptible Digital Image Steganography (Doctoral dissertation, Universiti Sains Malaysia).

Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. IETE Technical Review, 30(4), 344-358.

Atee, H. A. (2017). Extreme Learning Machine For Cryptography And Steganography Systems.

Bae, H., Jung, D., & Yoon, S. (2019). AnomiGAN: Generative adversarial networks for anonymizing private medical data. arXiv preprint arXiv:1901.11313.

Bai, J., Chang, C. C., Nguyen, T. S., Zhu, C., & Liu, Y. (2017). A high payload steganographic algorithm based on edge detection. Displays, 46, 42-51.

Bajpai, S., & Saxena, K. (2016). Evaluating Data Compression and Image Steganography Techniques for Optimized Embedding. (4), 265–271.

Balkrishan, J., & Singh, A. P. (2016). Concealing data in a digital image with multilayer security. Multimedia Tools and Applications, 75(12), 7045-7063.

Banday, S. A., & Pandit, M. K. (2021). Texture maps and chaotic maps framework for secure medical image transmission. Multimedia Tools and Applications, 80(12), 17667-17683.

Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., & Dutta, P. (2014). A novel secure image steganography method based on chaos theory in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1), 11-22.

Banerjee, I., Bhattacharyya, S., & Sanyal, G. (2013). Hiding & analyzing data in image using extended PMM. Procedia Technology, 10, 157-166.

Bedi, P., Bansal, R., & Sehgal, P. (2013). Using PSO in a spatial domain based image hiding scheme with distortion tolerance. Computers & Electrical Engineering, 39(2), 640-654.

Bellon, E., Feron, M., Deprez, T., Reynders, R., & Van den Bosch, B. (2011). Trends in PACS architecture. European journal of radiology, 78(2), 199-204.

Bhagat, D., & Bhardwaj, R. (2019). A Survey on Medical Images for Reversible Data Hiding Techniques. In 2019 Amity International Conference on Artificial Intelligence (AICAI) (pp. 811-817). IEEE.

Bianchi, L., Dorigo, M., Gambardella, L. M., & Gutjahr, W. J. (2009). A survey on metaheuristics for stochastic combinatorial optimization. Natural Computing, 8(2), 239-287.

Bilal, M., Imtiaz, S., Abdul, W., & Ghouzali, S. (2013). Zero-steganography using dct and spatial domain. In 2013 ACS International Conference on Computer Systems and Applications (AICCSA) (pp. 1-7). IEEE.

Bin, L., & Yeganeh, M. S. (2012). Comparison for image edge detection algorithms. IOSR Journal of Computer Engineering, 2(6), 1-4.

Biswas, R., & Bandyapadhay, S. K. (2020). Random selection based GA optimization in 2D-DCT domain color image steganography. Multimedia Tools and Applications, 79(11), 7101-7120.

Blelloch, G. E. (2001). Introduction to data compression. Computer Science Department, Carnegie Mellon University.

Boato, G., Conotter, V., De Natale, F. G., & Fontanari, C. (2009). Watermarking robustness evaluation based on perceptual quality via genetic algorithms. IEEE transactions on information forensics and security, 4(2), 207-216.

Boonstra, S., van der Blom, K., Hofmeyer, H., & Emmerich, M. T. (2021). Hybridization of an evolutionary algorithm and simulations of co-evolutionary design processes for early-stage building spatial design optimization. Automation in Construction, 124, 103522.

Boyles, S. D. (2015). Basic Optimization Concepts CE 377K (p. 11).

Cayre, F., Fontaine, C., & Furon, T. (2005). Watermarking security part one: theory. In Security, Steganography, and Watermarking of Multimedia Contents VII(Vol. 5681, pp. 746-757). International Society for Optics and Photonics.

Chahal, P. K., Pandey, S., & Goel, S. (2020). A survey on brain tumor detection techniques for MR images. Multimedia Tools and Applications, 79(29), 21771-21814.

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern recognition, 37(3), 469-474)

Chandramouli, R., Kharrazi, M., & Memon, N. (2003). Image steganography and steganalysis: Concepts and practice. In International Workshop on Digital Watermarking (pp. 35-49). Springer, Berlin, Heidelberg.

Chandwadkar, R., Dhole, S., Gadewar, V., & Raut, D. , & Tiwaskar,S. A. (2016). Comparison of Edge Detection Techniques. In Proceedings of Sixth IRAJ International Conference, Pune, India. http://dx. doi. org/10.13140/RG (Vol. 2, No. 5036.7123).

Chang, C. C., Chen, G. M., & Lin, M. H. (2004). Information hiding based on search-order coding for VQ indices. Pattern Recognition Letters, 25(11), 1253-1261.

Chanu, Y. J., Singh, K. M., & Tuithung, T. (2012). Image steganography and steganalysis: A survey. International Journal of Computer Applications, 52(2).

Chao, R. M., Wu, H. C., Lee, C. C., & Chu, Y. P. (2009). A novel image data hiding scheme with diamond encoding. EURASIP Journal on Information Security, 2009(1), 658047.

Chapman, M., Davida, G. I., & Rennhard, M. (2001). A practical and effective approach to large-scale automated linguistic steganography. In International Conference on Information Security (pp. 156-165). Springer, Berlin, Heidelberg.

Cheddad, A. (2009). Steganoflage: a new image steganography algorithm (Doctoral dissertation, University of Ulster).

Cheddad, A., Condell, A. J., Curran, K., Kevitt, P. M. (2010). Survey and analysis of current methods. Signal Processing,. Digital Image Steganography, 90(3), 727–752.

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), 727-752.

Cho, S., Cha, B. H., Gawecki, M., & Kuo, C. C. J. (2013). Block-based image steganalysis: Algorithm and performance evaluation. Journal of Visual

Collins, J. C., & Agaian, S. S. (2014). Taxonomy for spatial domain LSB steganography techniques. In Mobile Multimedia/Image Processing, Security, and Applications 2014 (Vol. 9120, p. 912006). International Society for Optics and Photonics.

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2008). Digital watermarking and steganography. Morgan kaufmann.

Cruz-Piris, L., Marsa-Maestre, I. & Lopez-Carmona, M. A. (2019). A variable-length chromosome genetic algorithm to solve a road traffic coordination multi-path problem. IEEE Access, 7, 111968-111981.

Dagadu, J. C., & Li, J. (2018). Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. Multimedia Tools and Applications, 77(18), 24289-24312.

Dalal, M., & Juneja, M. (2019). A robust and imperceptible steganography technique for SD and HD videos. Multimedia Tools and Applications, 78(5), 5769-5789.

Das, S. (2016). Comparison of various edge detection technique. International Journal of Signal Processing, Image Processing and Pattern Recognition, 9(2), 143-158.

De León-Aldaco, S. E., Calleja, H., & Alquicira, J. A. (2015). Metaheuristic optimization methods applied to power converters: A review. IEEE Transactions on Power Electronics, 30(12), 6791-6803

Desai, L., & Mali, S. (2018). Crypto-Stego-Real-Time (CSRT) System for Secure Reversible Data Hiding. VLSI Design, 1-8.

Despotović, I., Goossens, B., & Philips, W. (2015). MRI segmentation of the human brain: challenges, methods, and applications. Computational and mathematical methods in medicine, 2015.

Dhar, M., & Banerjee, S. (2019). An Efficient and Enhanced Mechanism for Message Hiding Based on Image Steganography Using ECC-Cryptosystem. In Advances in Communication, Devices and Networking (pp. 461-472). Springer, Singapore.

Dhiman, G., & Kaur, A. (2018). Optimizing the design of airfoil and optical buffer problems using spotted hyena optimizer. Designs, 2(3), 28.

Dilpreet, K., & Kaur, Y. (2014). Various image segmentation techniques: a review. International Journal of Computer Science and Mobile Computing, 3(5), 809-814.

Din, R., Utama, S., & Mustapha, A. (2018). Evaluation Review on Effectiveness and Security Performances of Text Steganography Technique. Indonesian Journal of Electrical Engineering and Computer Science, 11(2), 747-754.

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing, 2012(1), 25.

Doğan, Ş. (2016). A new data hiding method based on chaos embedded genetic algorithm for color image. Artificial Intelligence Review, 46(1), 129-143.

Dooley, J. F. (2016). Review of prisoners, lovers, & spies by Kristie Macrakis.

El_Rahman, S. A. (2018). A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. Computers & Electrical Engineering, 70, 380-399.

Elgabar, E. E. A., & Alamin, H. A. A. (2013). Comparison of LSB Steganography in GIF and BMP Images. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231-2307.

Elshare, S., & El-Emam, N. N. (2018). Modified Multi-Level Steganography to Enhance Data Security. International Journal of Communication Networks and Information Security, 10(3), 509.

Elshoush, H. T., Ali, I. A., Mahmoud, M. M., & Altigani, A. (2021). A Novel Approach to Information Hiding Technique using ASCII Mapping Based Image Steganography.

Eltyeb, E., & bed Elgabar, A. (2013). Comparison of LSB Steganography in BMP and JPEG Images. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231-2307.

Eslami, M., Shareef, H., & Mohamed, A. (2011). Application of artificial intelligent techniques in PSS design: a survey of the state-of-the-art methods. Przegląd Elektrotechniczny (Electrical Review), 87(4), 188-197.

Essa, R. J., Abdulah, N. A., & Al-Dabbagh, R. D. (2018). Steganography Technique using Genetic Algorithm. Iraqi Journal of Science, 59(3A), 1312-1325.

Fadhil, A. M. (2016). Bit Inverting Map Method for Improved Steganography Scheme (Doctoral Dissertation, Universiti Teknologi Malaysia).

Fatehi, F., & Wootton, R. (2012). Telemedicine, telehealth or e-health? A bibliometric analysis of the trends in the use of these terms. Journal of telemedicine and telecare, 18(8), 460-464.

Fawzi, A., Achuthan, A., & Belaton, B. (2021). Brain image segmentation in recent years: A narrative review. Brain Sciences, 11(8), 1055.

Ferreira, A. M. (2015). an overview on hiding and detecting stego-data in video streams. University of Amsterdam. System & Network Engineering–Research Project II.

Filler, T., Ker, A. D., & Fridrich, J. (2009). The square root law of steganographic capacity for Markov covers. In Media Forensics and Security (Vol. 7254, p. 725408). International Society for Optics and Photonics.

Foster, B., Bagci, U., Mansoor, A., Xu, Z., & Mollura, D. J. (2014). A review on segmentation of positron emission tomography images. Computers in biology and medicine, 50, 76-96.

Fridrich, J., & Lisonek, P. (2007). Grid colorings in steganography. IEEE Transactions on Information Theory, 53(4), 1547-1549.

Fridrich, J., Goljan, M., & Hogea, D. (2002). Steganalysis of JPEG images: Breaking the F5 algorithm. In International Workshop on Information Hiding (pp. 310-323). Springer, Berlin, Heidelberg.

Fridrich, J., Lisoněk, P., & Soukal, D. (2006). On steganographic embedding efficiency. In International Workshop on Information Hiding (pp. 282-296). Springer, Berlin, Heidelberg.

Fridrich, J., Pevný, T., & Kodovský, J. (2007). Statistically undetectable jpeg steganography: dead ends challenges, and opportunities. In Proceedings of the 9th workshop on Multimedia & security (pp. 3-14). ACM.

Gajabe, R., & Ali, S. T. (2022). Secret Key-Based Image Steganography in Spatial Domain. International Journal of Image and Graphics, 22(02), 2250014.

Gandomi, A. H., Yang, X. S., Talatahari, S., & Alavi, A. H. (2013). Metaheuristic algorithms in modeling and optimization. Metaheuristic applications in structures and infrastructures, 1-24.

Ganesan, P., & Bhavani, R. (2013). A High Secure and robust Image Steganography using Dual wavelet and blending Model. JCS, 9(3), 277-284.

Gaurav, K., & Ghanekar, U. (2018). Image steganography based on Canny edge detection, dilation operator and hybrid coding. Journal of Information Security and Applications, 41, 41-51.

Gayathri, C., & Kalpana, V. (2013). Study on image steganography techniques. International Journal of Engineering and Technology (IJET), 5(2), 572-577.

Gen, M., & Lin, L. (2007). Genetic Algorithms. Wiley Encyclopedia of Computer Science and Engineering, 1-15.

Gendreau, M., & Potvin, J. (2014). Tabu Search. In E. K. Burke & G. Kendall (Eds.), Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques (pp. 243–263). Boston, MA: Springer.

Ghebleh, M., & Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898-1907.

Glover, F. (1986). Future paths for integer programming and links to artificial intelligence. Computers & operations research, 13(5), 533-549.

Glover, F., & Martı, R. (2006). Metaheuristic Procedures for Training Neural Networks, chapter Tabu Search.

Glover, F., Laguna, M., & Martí, R. (2018). Principles and strategies of tabu search. In Handbook of Approximation Algorithms and Metaheuristics, Second Edition (pp. 361-377). Chapman and Hall/CRC.

Gordillo, N., Montseny, E., & Sobrevilla, P. (2013). State of the art survey on MRI brain tumor segmentation. Magnetic resonance imaging, 31(8), 1426-1438.

Graham, R. N., Perriss, R. W., & Scarsbrook, A. F. (2005). DICOM demystified: a review of digital file formats and their use in radiological practice. Clinical radiology, 60(11), 1133-1140.

Gupta, A. (2015). Application Of Steganography In Medical Images.

Gupta, R., Kumar, M., & Bathla, R. (2016). Data Compression-Lossless and Lossy Techniques. International Journal of Application or Innovation in Engineering & Management, 5(7), 120-125.

Gupta, S., & Mazumdar, S. G. (2013). Sobel edge detection algorithm. International journal of computer science and management Research, 2(2), 1578-1583.

Gutte, R. S., Chincholkar, Y. D., & Lahane, P. U. (2013). Steganography for two and three LSBS using extended substitution algorithm. ICTACT Journal on communication technology, 4(01), 685-690.

Ha, V. P., Dao, T. K., Pham, N. Y., & Le, M. H. (2021). A Variable-Length Chromosome Genetic Algorithm for Time-Based Sensor Network Schedule Optimization. Sensors, 21(12), 3990.

Hameurlaine, M., & Moussaoui, A. (2019). Survey of brain tumor segmentation techniques on magnetic resonance imaging. Nano Biomed. Eng, 11(2), 178-191.

Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. International Journal of Computer Science and Security (IJCSS), 6(3), 168-187.

Handayanto, R. T., Guha, S., Tripathi, N. K., & Herlawati. (2018). Genetic algorithms with variable length chromosomes for high constraint problems in spatial data. Proceedings of the 3rd International Conference on Informatics and Computing, ICIC 2018, 1–5. https://doi.org/10.1109/IAC.2018.8780468

Hashim, M. M., Rahim, M. S. M., Johi, F. A., Taha, M. S., & Hamad, H. S. (2018). Performance evaluation measurement of image steganography techniques with analysis of lsb based on variation image formats. International Journal of Engineering & Technology, 7(4), 3505-3514.

Hashim, M., Rahim, M., Shafry, M., & Alwan, A. A. (2018). A Review And Open Issues Of Multifarious Image Steganography Techniques In Spatial Domain. Journal of Theoretical & Applied Information Technology, 96(4).

Hemanth, D. J., Umamaheswari, S., Popescu, D. E., & Naaji, A. (2016). Application of genetic algorithm and particle swarm optimization techniques for improved image steganography systems. Open Physics, 14(1), 452-462.

Hofbauer, H., & Uhl, A. (2016). Identifying deficits of visual security metrics for images. Signal Processing: Image Communication, 46, 60-75.

Holden, R. J., & Karsh, B. T. (2010). The technology acceptance model: its past and its future in health care. Journal of biomedical informatics, 43(1), 159-172.

Holotyak, T., Fridrich, J., & Voloshynovskyy, S. (2005). Blind statistical steganalysis of additive steganography using wavelet higher order statistics. In IFIP International Conference on Communications and Multimedia Security, (pp. 273-274, Springer.

Hong, W., Chen, T. S., & Luo, C. W. (2012). Data embedding using pixel value differencing and diamond encoding with multiple-base notational system. Journal of Systems and Software, 85(5), 1166-1175.

Hong, W., Pan, C. L., Chen, T. S., Ji, W. Y., & Wang, Y. K. (2011). A Novel Data Embedding Method for High Payload Using Improved Pixel Segmentation Strategy. In Electrical Power Systems and Computers (pp. 89-95). Springer, Berlin, Heidelberg.

Höschel, K., & Lakshminarayanan, V. (2019). Genetic algorithms for lens design: a review. Journal of Optics, 48(1), 134-144.

Hossain, K., & Parekh, R. (2016). An approach towards image, audio and video steganography. In 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) (pp. 302-307). IEEE.

Hu, D., Zhou, S., Shen, Q., Zheng, S., Zhao, Z., & Fan, Y. (2019). Digital Image Steganalysis Based on Visual Attention and Deep Reinforcement Learning. IEEE Access, 7, 25924-25935.

Huffman, D. A. (1952). A method for the construction of minimum-redundancy codes. Proceedings of the IRE, 40(9), 1098-1101.

Hussain, H. S., Din, R., & Idrus, R. (2018). Preserve Imperceptibility and Robustness Performance on Steganography Technique based on StegaSVM-Shifted LBS Model. In Journal of Physics: Conference Series (Vol. 1018, No. 1, p. 012009). IOP Publishing.

Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques.

Hussain, M., Abdul Wahab, A., Javed, N., & Jung, K. H. (2016). Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. Symmetry, 8(6), 41.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66.

Hussein, Q. M. (2020). New Metrics for Steganography Algorithm Quality. International Journal of Advanced Science and Technology, 29(02).

Islam, M. N., Islam, M. F., & Shahrabi, K. (2015). Robust information security system using steganography, orthogonal code and joint transform correlation. Optik, 126(23), 4026-4031.

Iyer, S. S., & Laktharia, K. (2016). New robust and secure alphabet pairing text steganography algorithm. International Journal of Current Trends in Engineering & Research (IJCTER), 2(7), 15-21.

Jadwa, S. K. (2016). Canny Edge Detection Method for Medical Image Retrieval. International Journal of Scientific Engineering and Applied Science, 2(8), 54-59.

Jagadeesh, K., & Rajendran, A. (2019). Image Segmentation Techniques Implemented in Medical Images-A Research Review. Indian Journal of Public Health Research & Development, 10(2), 1091-1096.

Jain, M., & Lenka, S. K. (2016). Diagonal queue medical image steganography with Rabin cryptosystem. Brain informatics, 3(1), 39.

Jain, M., Choudhary, R. C., & Kumar, A. (2016). Secure medical image steganography with RSA cryptography using decision tree. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 291-295). IEEE.

Jain, N., Meshram, S., & Dubey, S. (2012). Image Steganography Using LSB and Edge–Detection Technique. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 223.

Jansi, K. R., & Muthusamy, S. H. (2020). Steganographic Approach to Enhance Secure Data Communication Using Nonograms. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 701-712). Springer, Singapore.

Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011). Information hiding using audio steganography–a survey. The International Journal of Multimedia & Its Applications (IJMA) Vol, 3, 86-96.

Jeevitha, K., Iyswariya, A., RamKumar, V., Basha, S. M., & Kumar, V. P. (2020). A review on various segmentation techniques in image processsing. European Journal of Molecular & Clinical Medicine, 7(4), 1342-1348.

Jeevitha, S., & Amutha Prabha, N. (2018). A comprehensive review on steganographic techniques and implementation. ARPN Journal of Engineering and Applied Sciences, 13, 17.

Ji, R., Yao, H., Liu, S., Wang, L., & Sun, J. (2006). A new steganalysis method for adaptive spread spectrum steganography. In 2006 international conference on intelligent information hiding and multimedia (pp. 365-368). IEEE.

Jiang, H., Yang, X., Yin, K., Zhang, S. & Cristoforo, J. A. (2011). Multi-path QoS-aware web service composition using variable length chromosome genetic algorithm. Information Technology Journal, 10(1), 113-119.

Joshi, K., Gill, S., & Yadav, R. (2018). A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. Journal of Computer Networks and Communications, 2018.

Jude Hemanth, D., Anitha, J., Popescu, D. E., & Son, L. H. (2018). A modified genetic algorithm for performance improvement of transform based image steganography systems. Journal of Intelligent & Fuzzy Systems, 35(1), 197-209.

Juneja, M. (2014). A Covert Communication Model-Based on Image Steganography. International Journal of Information Security and Privacy (IJISP), 8(1), 19-37.

Jung, K. H., & Yoo, K. Y. (2015). High-capacity index based data hiding method. Multimedia Tools and Applications, 74(6), 2179-2193.

Kaddouri, Z., & Omary, F. (2017). Application of the tabu search algorithm to cryptography. International Journal of Advanced Computer Science and Applications, 8(7), 82-87.

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326.

Kadhim, N. H., & Mosa, Q. (2021). Review Optimized Artificial Neural Network by Meta-Heuristic Algorithm and its Applications. Journal of Al-Qadisiyah for computer science and mathematics, 13(3), Page-34.

Kamau, G. M. (2014). An enhanced least significant bit steganographic method for information hiding (Doctoral dissertation).

Kanan, H. R., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications, 41(14), 6123-6130.

Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. Journal of information security and applications, 40, 217-235.

Karawia, A. A. (2021). Medical image steganographic algorithm via modified LSB method and chaotic map. IET Image Processing, 15(11), 2580-2590.

Karmakar, R., & Basu, A. (2019). Implementation of a Reversible Watermarking Technique for Medical Images. In Intelligent Innovations in Multimedia Data Engineering and Management (pp. 1-37). IGI Global.

Kasapbas¸I, M. C., & Elmasry, W. (2018). New LSB-based color image steganography method to enhance the efficiency in payload capacity, security and integrity check. Sadhana - Academy Proceedings in Engineering Sciences, 43(5). https://doi.org/10.1007/s12046-018-0848-4

Katzenbeisser, S. & Petitcolas, F. A. P. (2000) Information Hiding Techniques for Steganography and Digital Watermarking, Artech House.

Katzenbeisser, Stefan & Petitcolas, Fabien. (2015). Information hiding.

Kaur, H., & Singh, I. (2016). The Study Edge Detection of Medical Images using Transformation Techniques and Filteration Methods. International Journal of Computer Applications, 146(12), 39-42.

Kaur, N., & Behal, S. (2014). A Survey on various types of Steganography and Analysis of Hiding Techniques. International journal of engineering trends and technology, 11(8), 388-392.

Kaur, S., & Singh, I. (2016). Comparison of Edge Detection Techniques for Iris Recognition. International Journal of Computer Applications, 149(9), 42-47.

Khaleel, A. H., & Abduljaleel, I. Q. (2021). Secure image hiding in speech signal by steganography-mining and encryption. Indonesian Journal of Electrical Engineering and Computer Science, 21(3), 1692-1703.

Khalil, M. I. (2017). Medical image steganography: Study of medical image quality degradation when embedding data in the frequency domain. International Journal of Computer Network and Information Security, 9(2), 22.

Khalind, O. S. (2015). New methods to improve the pixel domain steganography, steganalysis, and simplify the assessment of steganalysis tools (Doctoral dissertation, University of Portsmouth).

Khalind, O., & Aziz, B. (2014). Detecting 2LSB steganography using extended pairs of values analysis. In Mobile Multimedia/Image Processing, Security, and Applications 2014 (Vol. 9120, p. 912003). International Society for Optics and Photonics.

Khalind, O., & Aziz, B. (2015). LSB steganography with improved embedding efficiency and undetectability. Computer Science & Information Technology, 5(1), 89-105.

Khan, S., Ahmad, N., & Wahid, M. (2016). Varying index varying bits substitution algorithm for the implementation of VLSB steganography. Journal of the Chinese Institute of Engineers, 39(1), 101-109.

Khan, S., Ahmad, N., Ismail, M., Minallah, N., & Khan, T. (2015, December). A secure true edge based 4 least significant bits steganography. In 2015 International Conference on Emerging Technologies (ICET) (pp. 1-4). IEEE.

Khatter, A., Browne, A., Singh, A., Dutta, M. K., Riha, K., & Burget, R. (2018). Generation of SVD Based Non-informative Unique ID for Authentication of MRI Images. In 2018 41st International Conference on Telecommunications and Signal Processing (TSP) (pp. 1-5). IEEE.

Kini, N. G., & Kini, V. G. (2019). A secured steganography algorithm for hiding an image in an image. In Integrated Intelligent Computing, Communication and Security (pp. 539-546). Springer, Singapore.

Kipper, G. (2004). Investigator's guide to steganography. Florida, CRC Press LLC.

Kolli, V. M., & Vaishakh, B. N. (2013). Key Based Data Embedding Technique in Image Steganography. 1–5.

Koohestani, B. (2020). A crossover operator for improving the efficiency of permutation-based genetic algorithms. Expert Systems with Applications, 151, 113381.

Koppu, S., & Viswanatham, V. M. (2018). Medical image security enhancement using two dimensional chaotic mapping optimized by self-adaptive grey wolf algorithm. Evolutionary Intelligence, 11(1-2), 53-71.

Kulkarni, A. J., Krishnasamy, G., & Abraham, A. (2017). Cohort intelligence: a socio-inspired optimization method. Switzerland: Springer International Publishing.

Kumar, K., Li, J. P., & Khan, S. A. (2015). Comparative study on various edge detection techniques for 2-D image. International Journal of Computer Applications, 119(22).

Kumar, M., Mittal, M. L., Soni, G., & Joshi, D. (2019). A tabu search algorithm for simultaneous selection and scheduling of projects. In Harmony search and nature inspired optimization algorithms (pp. 1111-1121). Springer, Singapore.

Kumar, R., & Singh, A. J. (2015). Understanding steganography over cryptography and various steganography techniques. International Journal of Computer Science and Mobile Computing, 4(3), 253-258.

Kumar, S., & Muttoo, S. K. (2013). A comparative study of image steganography in wavelet domain. A Monthly Journal of Computer Science and Information Technology, 2(2), 91-101.

Kumar, S., Singh, A., & Kumar, M. (2019). Information hiding with adaptive steganography based on novel fuzzy edge identification. Defence Technology, 15(2), 162-169.

Kumar, V., & Kumar, D. (2018). A modified DWT-based image steganography technique. Multimedia Tools and Applications, 77(11), 13279-13308.

Kuo, W. C., Kuo, S. H., & Wuu, L. C. (2015). Multi-bit data hiding scheme for compressing secret messages. Applied Sciences, 5(4), 1033-1049.

Laskar, S. A., & Hemachandran, K. (2012). High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6), 57.

Laskar, S. A., & Hemachandran, K. (2012). Secure data transmission using steganography and encryption. International Journal on Cryptography and Information Security, 2(3), 161-172.

Lawal, H. D., Adeyanju, I. A., Omidiora, E. O., Arulogun, O. T., & Omotosho, O. I. (2014). University examination timetabling using Tabu Search. International Journal of Scientific and Engineering Research, 5, 10.

Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172

Li, Q., Yu, C., & Chu, D. (2006). A robust image hiding method based on sign embedding and fuzzy classification. In 2006 6th World congress on intelligent control and automation (Vol. 2, pp. 10050-10053). IEEE.

Li, S. (2005). Study of steganographic techniques for digital images, (Master dissertation, City University of Hong Kong).

Li, S., Lv, H., Xu, C., Chen, T., & Zou, C. (2020). Optimized Train Path Selection Method for Daily Freight Train Scheduling. IEEE Access, 8, 40777-40790.

Lim, K. Y., & Mandava, R. (2018). A multi-phase semi-automatic approach for multisequence brain tumor image segmentation. Expert systems with applications, 112, 288-300.

Lin, B., & Miller, D. C. (2004). Tabu search algorithm for chemical process optimization. Computers & Chemical Engineering, 28(11), 2287-2306.

Lin, C. C. (2011). An information hiding scheme with minimal image distortion. Computer Standards & Interfaces, 33(5), 477-484.

Liu, Y., Qu, X., & Xin, G. (2016). A ROI-based reversible data hiding scheme in encrypted medical images. Journal of Visual Communication and Image Representation, 39, 51-57.

Loan, N. A., Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Bhat, G. M. (2017). Hiding electronic patient record (epr) in medical images: A high capacity and computationally efficient technique for e-healthcare applications. Journal of biomedical informatics, 73, 125-136.

Lu, C. S. (Ed.). (2004). Multimedia security: steganography and digital watermarking techniques for protection of intellectual property: steganography and digital watermarking techniques for protection of intellectual property. Igi Global.

Luo, X. Y., Wang, D. S., Wang, P., & Liu, F. L. (2008). A review on blind detection for image steganography. Signal Processing, 88(9), 2138-2157.

Mabrouk, F. A. (2017). Database Hiding in Tag Web Using Steganography by Genetic Algorithm (Doctoral dissertation, National Ribat University).

Madoš, B., Hurtuk, J., Čopjak, M., Hamaš, P., & Ennert, M. (2014). Steganographic algorithm for information hiding using scalable vector graphics images. Acta Electrotechnica et Informatica, 14(4), 42-45.

Mahalakshmi, V., Satheeshkumar, S., & Sivakumar, S. (2017). Performance of steganographic methods in medical imaging. International Journal of Computational and Applied Mathematics, 12(1), 2017.

Mahdi, M. H., Abdulrazzaq, A. A., Rahim, M. S. M., Taha, M. S., Khalid, H. N., & Lafta, S. A. (2019, May). Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. In IOP Conference Series: Materials Science and Engineering (Vol. 518, No. 5, p. 052002). IOP Publishing.

Mahmoud, M. M., & Elshoush, H. T. (2022). Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography–An Innovative Approach. IEEE Access, 10, 29954-29971.

Maini, R., & Aggarwal, H. (2008). Study and comparison of various image edge detection techniques. International journal of image processing (IJIP), 3(1).

Maniriho, P., & Ahmad, T. (2018). Enhancing the Capability of Data Hiding Method Based on Reduced Difference Expansion. Engineering Letters, 26(1).

Manisha, S., & Sharmila, T. S. (2018). Recognition of Characters in a Securely Transmitted Medical Image. In International conference on Computer Networks, Big data and IoT (pp. 286-292). Springer, Cham.

Manjarres, D., Landa-Torres, I., Gil-Lopez, S., Del Ser, J., Bilbao, M. N., Salcedo-Sanz, S., & Geem, Z. W. (2013). A survey on applications of the harmony search algorithm. Engineering Applications of Artificial Intelligence, 26(8), 1818-1831.

Mantos, P. L., & Maglogiannis, I. (2016). Sensitive patient data hiding using a ROI reversible steganography scheme for DICOM images. Journal of medical systems, 40(6), 156.

Mariam, O. (2017). An Improved Image Steganography Based On Least Significant Bit Matching Revisited (Lsbmr) Using Sobel Edge Detection.

Mathivanan, P., Jero, S. E., Ramu, P., & Ganesh, A. B. (2018). QR code based patient data protection in ECG steganography. Australasian physical & engineering sciences in medicine, 41(4), 1057-1068.

Mehta, D. M., & Bhatti, D. G. (2019). Research review on digital image steganography which resists against compression. Emerging Trends in Expert Applications and Security, 529-534.

Memari, A., Ahmad, R., & Rahim, A. R. A. (2017). Metaheuristic algorithms: guidelines for implementation. Journal of Soft Computing and Decision Support Systems, 4(6), 1-6.

Mishra, M., Tiwari, G., & Yadav, A. K. (2014). Secret communication using public key steganography. In International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014) (pp. 1-5). IEEE.

Modi, M. R., Islam, S., & Gupta, P. (2013). Edge based steganography on colored images. In International Conference on Intelligent Computing (pp. 593-600). Springer, Berlin, Heidelberg.

Mohamed, H. M., Ali, A. F., & Altaweel, G. S. (2017). A hybrid curvelet transform and genetic algorithm for image steganography. International Journal of Advanced Computer Science and Applications, 8(8), 2017.

Mohamed, M. A. (2018). Steganography for Better Data Integrity and Privacy (Doctoral dissertation, Utica College).

Mohamed, M. H., & Mohamed, L. M. (2016). High capacity image steganography technique based on LSB substitution method. Applied Mathematics & Information Sciences, 10(1), 259.

Mohamed, M., Al-Afari, F., & Bamatraf, M. A. (2011). Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. Int. Arab. J. e Technol., 2(1), 11-17.

Mohammed, G. N. (2015). An enhanced method based on intermediate significant bit technique for watermark images (Doctoral dissertation, Universiti Utara Malaysia).

Mohammed, G. N., Yasin, A., & Zeki, A. M. (2012). Digital image watermarking, analysis of current methods. In 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT) (pp. 324-329). IEEE.

Mohammed, G. N., Yasin, A., & Zeki, A. M. (2013). High Watermarking Image Quality Based on Dual Intermediate Significant Bit (DISB). International Journal of Digital Content Technology and Its Applications, 7(5), 733–742. https://doi.org/10.4156/jdcta.vol7.issue5.86

Mohammed, G. N., Yasin, A., & Zeki, A. M. (2013). Trade-off between Robustness and Quality Based on Dual Intermediate Significant Bits. In 2013 International Conference on Advanced Computer Science Applications and Technologies (pp. 186-191). IEEE.

Mohammed, G. N., Yasin, A., & Zeki, A. M. (2014). Robust image watermarking based on Dual Intermediate Significant Bit (DISB). In 6th International Conference on Computer Science and Information Technology (CSIT) (pp. 18-22). IEEE.

Mondal, S., Debnath, R., & Mondal, B. K. (2016). An improved color image steganography technique in spatial domain. In 2016 9th International Conference on Electrical and Computer Engineering (ICECE) (pp. 582-585). IEEE.

Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R. (2014). Watermarking techniques used in medical images: a survey. Journal of digital imaging, 27(6), 714-729.

Mu'ath Al-Shaikh. (2017). Medical image content protection by secret information hiding to support telemedicine. (Protection des contenus des images médicales par camouflage d'informations secrètes pour l'aide à la télémédecine)(Doctoral dissertation, University of Western Brittany, France).

Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W. (2015). A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS, 9(5), 1938-1962.

Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Qureshi, R. J. (2015). A secure cyclic steganographic technique for color images using randomization. arXiv preprint arXiv:1502.07808.

Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. (2017). CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications, 76(6), 8597-8626.

Muhammad, K., Sajjad, M., & Baik, S. W. (2016). Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy. Journal of medical systems, 40(5), 114.

Mungmode, S., Sedamkar, R. R., & Kulkarni, N. (2016). An Enhanced Edge Adaptive Steganography Approach using Threshold Value for Region Selection. arXiv preprint arXiv:1601.02076.

Mustra, M., Delac, K., & Grgic, M. (2008). Overview of the DICOM standard. In 2008 50th International Symposium ELMAR (Vol. 1, pp. 39-44). IEEE.

Nabi, F., & Afzal, M. M. (2020). Image Steganography: Critical Findings through Some Novel Technique. International Journal of Innovative Technology and Exploring Engineering, 9(5), 878–890. https://doi.org/10.35940/ijitee.e2634.039520.

Nagaraju, C., & ParthaSarathy, S. S. (2014). Embedding patient information in medical images using LBP and LTP. Circuits and Systems: An International Journal, 1(1), 39-48.

Nayak, J., Bhat, P. S., Acharya, R., & Kumar, M. S. (2009). Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes. Journal of medical systems, 33(3), 163-171.

Nikolic, M., Tuba, E., & Tuba, M. (2016). Edge detection in medical ultrasound images using adjusted Canny edge detection algorithm. In 2016 24th Telecommunications Forum (TELFOR) (pp. 1-4). IEEE.

Nipanikar, S. I., & Deepthi, H. (2019). Enhanced whale optimization algorithm and wavelet transform for image steganography. Multimedia Research (MR), 2(3), 23-32.

Nipanikar, S. I., & Deepthi, V. H. (2016). A multiple criteria-based cost function using wavelet and edge transformation for medical image steganography. Journal of Intelligent Systems, 27(3), 331-347.

Nissar, A., & Mir, A. H. (2010). Classification of steganalysis techniques: A study. Digital Signal Processing, 20(6), 1758-1770.

Norouzi, A., Rahim, M. S. M., Altameem, A., Saba, T., Rad, A. E., Rehman, A., & Uddin, M. (2014). Medical image segmentation methods, algorithms, and applications. IETE Technical Review, 31(3), 199-213.

Nosrati, M., & Karimi, R. (2012). A survey on usage of genetic algorithms in recent steganography researches. World Applied Programming, 2(3), 206-210.

Nuryanti, L. (2021). A VEHICLE ROUTING PROBLEM OPTIMIZATION WITH DRONE USING TABU SEARCH ALGORITHM AND ANALYTICAL HIERARCHY PROCESS. Majalah Ilmiah Pengkajian Industri, 15(1).

Nyeem, H., Boles, W., & Boyd, C. (2013). A review of medical image watermarking requirements for teleradiology. Journal of digital imaging, 26(2), 326-343.

Obaid, A. H. (2015). Information hiding techniques for steganography and digital watermarking. UDC 681.518 (04) Interactive Systems: Problems of Human-Computer Interaction.–Collection of scientific papers.− Ulyanovsk: USTU, 2015. 63-70.

Ogundokun, R. O., Abikoye, O. C., Misra, S., & Awotunde, J. B. (2020, November). Modified least significant bit technique for securing medical images. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 553-565). Springer, Cham.

Oktavianto, B., Purboyo, T. W., & Saputra, R. E. (2017). A Proposed Method for Secure Steganography on PNG Image Using Spread Spectrum Method and Modified Encryption. International Journal of Applied Engineering Research, 12(21), 10570-10576.

Olanrewaju, R. F., Ali, N. A. B., Khalifa, O., & Manaf, A. A. (2013). ICT in Telemedicine: conquering privacy and security issues in health care services. electronic Journal of Computer Science and Information Technology (eJCSIT), 4(1), 19-24.

Olanrewaju, R. F., Khalifa, O. O., Hashim, A. H., Zeki, A. M., & Aburas, A. A. (2011). Forgery detection in medical images using complex valued neural network (CVNN). Australian Journal of Basic and Applied Sciences, 5(7), 1251-1264.

Onyeator, I., & Okpara, N. (2019). Human Communication in a Digital Age: Perspectives on Interpersonal communication in the family. New Media and Mass Communication, 78, 35-45.

Pai, P. Y., Chang, C. C., Chan, Y. K., & Liu, C. M. (2012). An ROI-based medical image hiding method. Int. J. Innov. Comput. Inf. Control, 1(8), 4521-4533.

Pandey, H. M. (2020). Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Future Generation Computer Systems, 111, 213-225.

Parah, S. A., Akhoon, J. A., Sheikh, J. A., Loan, N. A., & Bhat, G. M. (2015). A high capacity data hiding scheme based on edge detection and even-odd plane separation. In 2015 Annual IEEE India Conference (INDICON) (pp. 1-5). IEEE.

Parah, S. A., Sheikh, J. A., & Bhat, G. M. (2012). Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique. In 2012 International Conference on Emerging Trends in Science, Engineering and Technology (INCOSET) (pp. 192-197). IEEE.

Parah, S. A., Sheikh, J. A., & Bhat, G. M. (2012). High capacity data embedding using joint Intermediate Significant Bit (ISB) and Least Significant Bit (LSB) technique. J Inf Eng Appl, ISSN (Paper), 2224-5782.

Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A., & Bhat, G. M. (2017). Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications, 76(8), 10599-10633.

Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Loan, N. A. (2018). Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. Future Generation Computer Systems.

Parah, S. A., Sheikh, J. A., Akhoon, J. A., Loan, N. A., & Bhat, G. M. (2018). Information hiding in edges: A high capacity information hiding technique using hybrid edge detection. Multimedia Tools and Applications, 77(1), 185-207.

Patil, D. D., & Deore, S. G. (2013). Medical image segmentation: a review. International Journal of Computer Science and Mobile Computing, 2(1), 22-27.

Peng, J., Li, H., Jiang, Q., Wang, Y., & Chen, J. (2014). An integrative approach for measuring semantic similarities using gene ontology. BMC systems biology, 8(5), 1-12.

Pevný, T., Filler, T., & Bas, P. (2010). Using high-dimensional image models to perform highly undetectable steganography. In International Workshop on Information Hiding (pp. 161-177). Springer, Berlin, Heidelberg.

Pham, D. T., & Castellani, M. (2014). Benchmarking and comparison of nature-inspired population-based continuous optimization algorithms. Soft Computing, 18(5), 871-903.

Pharwaha, A. P. S. (2010). Secure data communication using moderate bit substitution for data hiding with three layer security. IE (I) Journal-ET, 91, 45-50.

Phonsa, G., & Bansal, K. K. (2018). A Comprehensive Review of Soft Computing Techniques. International Journal of Applied Engineering Research, 13(11), 9881-9886.

Pibre, L., Pasquet, J., Ienco, D., & Chaumont, M. (2016). Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover sourcemismatch. Electronic Imaging, 2016(8), 1-11.

Poornima, R., & Iswarya, R. J. (2013). An overview of digital image steganography. International Journal of Computer Science and Engineering Survey, 4(1), 23.

Prabakaran, G., & Bhavani, R. (2012). A modified secure digital image steganography based on Discrete Wavelet Transform. In 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)(pp. 1096-1100). IEEE.

Prabhu, P., & Manjunath, K. N. (2019). Secured Image Transmission in Medical Imaging Applications—A Survey. In Computer Aided Intervention and Diagnostics in Clinical and Medical Images (pp. 125-133). Springer, Cham.

Pradhan, A., Sahu, A. K., Swain, G., & Sekhar, K. R. (2016). Performance evaluation parameters of image steganography techniques. In 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS) (pp. 1-8). IEEE.

Praneetha, S. R. (2015). Video stegenography by intermediate significant biplanes. International Journal of Computer Science and Information Technologies, 6(5), 4646-4650.

Priyadharshini, A., Umamaheswari, R., Jayapandian, N., & Priyananci, S. (2021, February). Securing medical images using encryption and LSB steganography. In 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-5). IEEE.

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE security & privacy, 1(3), 32-44.

Qasim, A. F. (2019). Reversible and imperceptible watermarking approach for ensuring the integrity and authenticity of brain MR images (Doctoral dissertation, University of Salford).

Qin, C., Chang, C. C., & Hsu, T. J. (2015). Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimedia Tools and Applications, 74(15), 5861-5872.

Qin, C., Chang, C. C., Huang, Y. H., & Liao, L. T. (2013). An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism. IEEE Transactions on Circuits and Systems for Video Technology, 23(7), 1109-1118.

Rabah, K. (2004). Steganography-the art of hiding data. Information Technology Journal, 3(3), 245-269.

Raftari, N., & Moghadam, A. M. E. (2012). Digital image steganography based on assignment algorithm and combination of DCT-IWT. In 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (pp. 295-300). IEEE.

Raghu, K., Faiyyaz, S. M., Halim, S. H., Sachin, & Das, R. (2021). Sparse Image Reconstruction by employing Adaptive Gradient Algorithm in Image Steganography Turkish Journal of Computer and Mathematics Education Research Article. 12(11), 4996–5004.

Rahman, S., Masood, F., Khan, W. U., Ullah, N., Khan, F. Q., Tsaramirsis, G., ... & Ashraf, M. (2020). A novel approach of image steganography for secure

communication based on LSB substitution technique. CMC-Comput Mater Continua, 64(1), 31-61.

Rahmat, R. F., Andreas, T. S. M., Fahmi, F., Pasha, M. F., Alzahrani, M. Y., & Budiarto, R. (2019). Analysis of DICOM Image Compression Alternative Using Huffman Coding. Journal of Healthcare Engineering, 2019.

Rai, P., Gurung, S., & Ghose, M. K. (2015). Analysis of image steganography techniques: a survey. International Journal of Computer Applications, 114(1).

Rajesh, k. & Singh, A. J. (2015). Understanding Steganography over Cryptography and Various Steganography Techniques, International Journal of Computer Science and Mobile Computing, 4(3), 253-258.

Rajesh, T., Karnan, M., & Sivakumar, R. (2014). Performance Analysis of Iris Recognition System-A Review. International Journal of Computer Science & Information Technology, 39-50.

Rakshit, P., Ganguly, S., Pal, S., Aly, A. A., & Le, D. (2021). Securing technique using pattern-Based LSB audio steganography and intensity-based visual cryptography. Computers, Materials & Continua, 67(1), 1207-1224.

Ramakrishnan, S. (2018). Cryptographic and Information Security Approaches for Images and Videos. CRC Press.

Ramu, P., & Swaminathan, R. (2016). Imperceptibility—robustness tradeoff studies for ECG steganography using continuous ant colony optimization. Expert Systems with Applications, 49, 123-135.

Ranjith Kumar, R., Jayasudha, S., & Pradeep, S. (2016). Efficient and secure data hiding in encrypted images: A new approach using chaos. Information Security Journal: A Global Perspective, 25(4-6), 235-246.

Rao, R. C., Jayasree, P. V. Y., Rao, S. S., & Kumar, P. M. (2021, August). Spread Spectrum Based Speech Steganography Using RDWT. In 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 927-933). IEEE.

Rashid, A., Salamat, N., & Prasath, V. (2018). An algorithm for data hiding in radiographic images and ePHI/R application. Technologies, 6(1), 7.

Rashid, R. D. (2015). Robust Steganographic Techniques for Secure Biometric-based Remote Authentication (Doctoral dissertation, University of Buckingham).

Ratib, O., Roduit, N., Nidup, D., De Geer, G., Rosset, A., & Geissbuhler, A. (2016). PACS for Bhutan: a cost-effective open source architecture for emerging countries. Insights into imaging, 7(5), 747-753.

Rong, W., Li, Z., Zhang, W., & Sun, L. (2014). An improved CANNY edge detection algorithm. In 2014 IEEE International Conference on Mechatronics and Automation (pp. 577-582). IEEE.

Roy, R., & Changder, S. (2016). Quality evaluation of image steganography techniques: a heuristics based approach. International Journal of Security and Its Applications, 10(4), 179-196.

Roy, R., & Laha, S. (2015). Optimization of stego image retaining secret information using genetic algorithm with 8-connected PSNR. Procedia Computer Science, 60, 468-477.

Roy, R., Changder, S., Sarkar, A., & Debnath, N. C. (2013). Evaluating image steganography techniques: Future research challenges. In 2013 International Conference on Computing, Management and Telecommunications (ComManTel) (pp. 309-314). IEEE.

Ryerkerk, M. L. (2018). Metameric representations in evolutionary algorithms (Doctoral dissertation, Michigan State University).

Ryerkerk, M., Averill, R., Deb, K., & Goodman, E. (2019). A survey of evolutionary algorithms using metameric representations. Genetic Programming and Evolvable Machines, 20(4), 441-478.

Sadiku, M. N. O., Adebo, P. O., & Ajayi-Majebi, A. (2021). AI in Computer Science A Primer (pp. 644–648).

Sagar, V., & Kumar, K. (2014). A symmetric key cryptographic algorithm using counter propagation network (cpn). In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (p. 51). ACM.

Salameh, J. N. B. (2019). A new approach for securing medical images and Patient's information by using a hybrid system. Int J of Computer Sci Netw Secur, 19(4), 28-39.

Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data security using cryptography and steganography techniques. International Journal of Advanced Computer Science and Applications, 7(6), 390-397.

Samidha, D., & Agrawal, D. (2013). Random image steganography in spatial domain. In 2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT)(pp. 1-3). IEEE.

Samima, S., Roy, R., & Changder, S. (2013). Secure key based image realization steganography. In 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013) (pp. 377-382). IEEE.

Santhi, G., & Adithya, B. (2017). A Survey On Medical Image Protection Using Various Steganography Techniques. Advances in Natural and Applied Sciences, 11(12), 89-95.

Sari, R. D., & Siahaan, A. P. U. (2018). Least Significant Bit Comparison between 1-bit and 2-bit Insertion. 110–113. https://doi.org/10.31227/osf.io/twmrn

Sarkar, T., & Sanyal, S. (2014). Digital Watermarking Techniques in Spatial and Frequency Domain. arXiv preprint arXiv:1406.2146.

Sayood, K. (2017). Introduction to data compression. Morgan Kaufmann.

Seyyedi, S. A., & Ivanov, N. N. (2014). High payload and secure steganography method based on block partitioning and integer wavelet transform.

Shah, P. D., & Bichkar, R. (2021). Genetic Algorithm-Based Imperceptible Image Steganography Technique with Histogram Distortion Minimization. In Proceedings of International Conference on Computational Intelligence, Data Science and Cloud Computing: IEM-ICDC 2020 (Vol. 62, p. 267). Springer Nature.

Shah, P. D., & Bichkar, R. S. (2018). A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator. In International Conference on Intelligent Computing and Applications (pp. 119-129). Springer, Singapore.

Shah, P. D., & Bichkar, R. S. (2019). Genetic Algorithm Based Imperceptible Spatial Domain Image Steganography Technique with High Payload Capacity. International Journal of Recent Technology and Engineering (IJRTE), 7(5).

Shaik, A., & Masilamani, V. (2015). A robust digital image watermarking based on singular value decomposition and tabu-search. The IIOAB Journal, 6(3), 1.

Shaik, A., Thanikaiselvan, V., & Amitharajan, R. (2017). Data security through data hiding in images: a review. Journal of Artificial Intelligence, 10(1), 1-21.

Shanthakumari, R., Devi, E. R., Rajadevi, R., & Bharaneeshwar, B. (2021, May). Information hiding in audio steganography using LSB matching revisited. In Journal of Physics: Conference Series (Vol. 1911, No. 1, p. 012027). IOP Publishing.

Sharif, A., Mollaeefar, M., & Nazari, M. (2017). A novel method for digital image steganography based on a new three-dimensional chaotic map. Multimedia Tools and Applications, 76(6), 7849-7867.

Sharma, U., Sood, M., & Puthooran, E. (2018). Lossless Compression of Medical Image Sequences Using a Resolution Independent Predictor and Block Adaptive

Encoding. International journal of electrical and computer engineering systems, 9(2), 69-79.

Shawkat, S. A. (2016). Enhancing Steganography Techniques in Digital Images (Doctoral dissertation, Faculty of Computers and Information, Mansoura University Egypt).

Shelke, S. G., & Jagtap, S. K. (2015). Analysis of spatial domain image steganography techniques. In 2015 International Conference on Computing Communication Control and Automation (pp. 665-667). IEEE.

Shi, Y. Q., Chen, C., Xuan, G., & Su, W. (2007). Steganalysis versus splicing detection. In International Workshop on Digital Watermarking (pp. 158-172). Springer, Berlin, Heidelberg.

Shibani, K., Kumar, K. S., & Shanmugam, G. S. (2020). An Effective Approach for Plant Monitoring, Classification and Prediction Using IoT and Machine Learning. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 143-154). Springer, Singapore.

Shibani, K., Sendhil Kumar, K. S., & Siva Shanmugam, G. (2020). An effective approach for plant monitoring, classification and prediction using iot and machine learning. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 143-154). Springer, Singapore.

Shih, F. Y. (2017). Digital watermarking and steganography: fundamentals and techniques. CRC press.

Shiva Kumar, K. B., Raja, K. B., Chhotaray, R. K., & Pattnaik, S. (2011, March). Integration of Spatial and Transform Domain in LSB Steganography. In International Conference on Advances in Communication, Network, and Computing (pp. 400-402). Springer, Berlin, Heidelberg.

Shokranipour, S., & Hasanzadeh, M. (2016). High capacity image steganography method by using Particle Swarm Optimization. The Modares Journal of Electrical Engineering, 15(4), 1-7.

Shrestha, S. M. S. C++ Implementation of Neural Cryptography for Public Key Exchange and Secure Message Encryption with Rijndael Cipher.

Shrivakshan, G. T., & Chandrasekar, C. (2012). A comparison of various edge detection techniques used in image processing. International Journal of Computer Science Issues (IJCSI), 9(5), 269.

Shukla, A. K., Singh, A., Singh, B., & Kumar, A. (2018). A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing. IEEE Access, 6, 51130-51139.

Siar, F., Alirezazadeh, S., & Jalali, F. (2018). A novel steganography approach based on ant colony optimization. In 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS) (pp. 215-219). IEEE.

Singh, A. K. (2015). Some New Techniques of Improved Wavelet Domain Watermarking ofr Medical Images.

Singh, A. K., Kumar, B., Singh, G., & Mohan, A. (2017). Medical image watermarking techniques: a technical survey and potential challenges. In Medical Image Watermarking (pp. 13-41). Springer, Cham.

Singh, B., & Kaur, J. (2015). Survey on steganography techniques for digital images 1, 2 CSE. IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India baljit. singh@ bbsbec. edu. in, IJESAT, 2(3).

Singh, J., Kaur, G., & Garcha, M. K. (2015). Review of Spatial and Frequency Domain Steganographic Approaches. International Journal of Engineering Research and Technology, 4(06).

Singh, S., & Singh, R. (2015). Comparison of various edge detection techniques. In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 393-396). IEEE.

Singla, D., & Juneja, M. (2014). An analysis of edge based image steganography techniques in spatial domain. In 2014 Recent Advances in Engineering and Computational Sciences (RAECS) (pp. 1-5). IEEE.

Sinha, B. (2015). Comparison of PNG & JPEG Format for LSB Steganography. International Journal of Science and Research, 4(4, 5), 198-201.

Snasel, V., Kromer, P., Safarik, J., & Platos, J. (2020). JPEG steganography with particle swarm optimization accelerated by AVX. Concurrency and Computation: Practice and Experience, 32(8), e5448.

Sorensen, K., Sevaux, M., & Glover, F. (2017). A history of metaheuristics. arXiv preprint arXiv:1704.00853.

Srayyih Almaliki, M. N. (2019). Multilevel secure digital image steganography framework using random function and advanced encryption standard. Journal of Computational and Theoretical Nanoscience, 16(11), 4812-4825.

Sridhar, B. (2019). Cross-Layered Embedding of Watermark on Image for High Authentication. Pattern Recognition and Image Analysis, 29(1), 194-199.

Stinson, D. R. (2005). Cryptography: theory and practice. Chapman and Hall/CRC.

Stringer, H. (2007). Behavior of variable-length genetic algorithms under random selection.

Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. Computer science review, 13, 95-113.

Subhedar, M. S., & Mankar, V. H. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. Computers & Electrical Engineering, 54, 406-422.

Subhedar, M. S., & Mankar, V. H. (2020). Secure image steganography using framelet transform and bidiagonal SVD. Multimedia Tools and Applications, 79(3), 1865-1886.

Sugathan, S. (2016). An improved LSB embedding technique for image steganography. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 609-612). IEEE.

Sun, S. (2016). A novel edge-based image steganography with 2k correction and Huffman encoding. Information Processing Letters, 116(2), 93-99.

Sun, Y. (2019). Evaluation methods of accuracy and reproducibility for image segmentation algorithms (Doctoral dissertation, University of Saskatchewan).

Swaraja, K. (2018). Medical image region based watermarking for secured telemedicine. Multimedia Tools and Applications, 77(21), 28249-28280.

Taha, M. S., Rahem, M. S. M., Hashim, M. M., & Khalid, H. N. (2022). High payload image steganography scheme with minimum distortion based on distinction grade value method. Multimedia Tools and Applications, 1-34.

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.

Taher, A. A., & Kadhim, S. M. (2019). Hybrid between genetic algorithm and artificial bee colony for key generation purpose. Journal of Al-Qadisiyah for computer science and mathematics, 11(4), Page-37.

Talbi, E. G. (2009). Metaheuristics: from design to implementation (Vol. 74). John Wiley & Sons.

Taleby Ahvanooey, M., Li, Q., Shim, H. J., & Huang, Y. (2018). A comparative analysis of information hiding techniques for copyright protection of text documents. Security and Communication Networks, 2018.

Thabit, R. (2021). Review of medical image authentication techniques and their recent trends. Multimedia Tools and Applications, 80(9), 13439-13473.

Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., Roslan, N. A., & Din, R. (2021). A comparative analysis of arabic text steganography. Applied Sciences, 11(15), 6851.

Thangadurai, K., & Devi, G. S. (2014). An analysis of LSB based image steganography techniques. In 2014 International Conference on Computer Communication and Informatics (pp. 1-4). IEEE.

Thiyagarajan, P., & Aghila, G. (2013). Reversible dynamic secure steganography for medical image using graph coloring. Health Policy and Technology, 2(3), 151-161.

Thiyagarajan, P., Aghila, G., & Venkatesan, V. P. (2011). Stego-Image Generator (SIG)-Building Steganography Image Database. In International Conference on Digital Image Processing and Information Technology (pp. 257-267). Springer, Berlin, Heidelberg.

Thongkor, K., & Amornraksa, T. (2017). An image watermarking method in HSL color model. In 2017 10th International Conference on Ubi-media Computing and Workshops (Ubi-Media) (pp. 1-6). IEEE.

Ting, T. O., Yang, X. S., Cheng, S., & Huang, K. (2015). Hybrid metaheuristic algorithms: past, present, and future. Recent advances in swarm intelligence and evolutionary computation, 71-83.

Tiwari, N., & Shandilya, D. M. (2010). Evaluation of various LSB based methods of image steganography on GIF file format. International Journal of Computer Applications, 6(2), 1-4.

Trivedi, S., & Chandramouli, R. (2003). Active steganalysis of sequential steganography. In Security and Watermarking of Multimedia Contents V (Vol. 5020, pp. 123-130). International Society for Optics and Photonics.

Tsafarakis, S., Zervoudakis, K., & Andronikidis, A. (2021). Optimal product line design using Tabu Search. Journal of the Operational Research Society, 1-12.

Ullagaddi, V., Hassan, F., Cameron, B. D., Nims, D., & Devabhaktuni, V. (2013). A new passcode-based approach for hiding classified information in images. In 45th Southeastern Symposium on System Theory (pp. 141-145). IEEE.

Upadhyay, & Kashyap, 2016). Fast Segmentation Methods for Medical Images. International Journal of Computer Applications, 156(3), 18-23.

Usha B., Srinath N., Narayan K., & Sangeetha K. (2014). A Secure Data Embedding Technique in Image Steganography for Medical Images. International Journal of Advanced Research in Computer and Communication Engineering. 3(8), 7753-7756.

Usman, M. A., & Usman, M. R. (2018). Using image steganography for providing enhanced medical data security. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-4). IEEE.

Usman, M. A., Shin, S. Y., Shahid, M., & Lövström, B. (2017). A no reference video quality metric based on jerkiness estimation focusing on multiple frame freezing in video streaming. IETE Technical Review, 34(3), 309-320.

Usman, M. A., Usman, M. R., & Shin, S. Y. (2017). Quality assessment for wireless capsule endoscopy videos compressed via HEVC: From diagnostic quality to visual perception. Computers in biology and medicine, 91, 112-134.

Uwaisy, M. A., Baizal, Z. K. A., & Reditya, M. Y. (2019). Recommendation of Scheduling Tourism Routes using Tabu Search Method (Case Study Bandung). Procedia Computer Science, 157, 150-159.

Venkateswarlu, C. (2021). A Metaheuristic Tabu Search Optimization Algorithm: Applications to Chemical and Environmental Processes.

Verma, V., & Chawla, R. (2014). An enhanced Least Significant Bit steganography method using midpoint circle approach. In 2014 International Conference on Communication and Signal Processing (pp. 105-108). IEEE.

Vico, J. U. D. (2010). Steganography And Steganlaysis: Data Hiding In Vorbis Audio Streams.

Wadhwa, A., Bhardwaj, A., & Verma, V. S. (2019). A review on brain tumor segmentation of MRI images. Magnetic resonance imaging, 61, 247-259.

Wang, D., Chen, D., Ma, B., Xu, L., & Zhang, J. (2017). A high capacity spatial domain data hiding scheme for medical images. Journal of Signal Processing Systems, 87(2), 215-227.

Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. Pattern recognition, 34(3), 671-683.

Wang, S., Yang, B., & Niu, X. (2010). A secure steganography method based on genetic algorithm. Journal of Information Hiding and Multimedia Signal Processing, 1(1), 28-35.

Wang, W., & Zhang, W. (2017). Huffman coding-based adaptive spatial modulation. IEEE Transactions on Wireless Communications, 16(8), 5090-5101.

Wang, Y. (2017). Solving the threat of LSB steganography within data loss prevention systems (Doctoral dissertation, University of St Andrews).

Watters, P. A., Martin, F., & Stripf, S. H. (2005). Visual steganalysis of LSB-encoded natural images. In Third International Conference on Information Technology and Applications (ICITA'05) (Vol. 1, pp. 746-751). IEEE.

Wayner, P. (2009). Disappearing cryptography: information hiding: steganography and watermarking. Morgan Kaufmann.

Wazirali, R. A. (2016). Optimization of perceptual steganography capacity using the human visual system and evolutionary computation (Doctoral dissertation).

Wazirali, R. A., Chaczko, Z., & Kale, A. (2014). Digital multimedia archiving based on optimization steganography system. In 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE) (pp. 82-86). IEEE.

Wazirali, R., Alasmary, W., Mahmoud, M. M., & Alhindi, A. (2019). An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms. IEEE Access, 7, 133496-133508.

Wilson, L. S., & Maeder, A. J. (2015). Recent directions in telemedicine: review of trends in research and practice. Healthcare informatics research, 21(4), 213-222.

Wu, C. C., Kao, S. J., & Hwang, M. S. (2011). A high-quality image sharing with steganography and adaptive authentication scheme. Journal of Systems and Software, 84(12), 2196-2207.

Wu, H. C., Lee, C. C., Tsai, C. S., Chu, Y. P., & Chen, H. R. (2009). A high capacity reversible data hiding scheme with edge prediction and difference expansion. Journal of Systems and Software, 82(12), 1966-1973.

Wu, H. C., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings-Vision, Image and Signal Processing, 152(5), 611-615.

Wu, H. T., Huang, J., & Shi, Y. Q. (2015). A reversible data hiding method with contrast enhancement for medical images. Journal of Visual Communication and Image Representation, 31, 146-153.

Yadav, E. R., Kumar, E. C., & Yadav, E. R. (2019). High Capacity Embedding And Secured Steganography Model By Using GA And Integer Wavelet Transform. image, 1.

Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Transactions on Information Forensics and Security, 3(3), 488-497.

Yang, Y., Zhang, W., Liang, D., & Yu, N. (2017). A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images. Multimedia Tools and Applications, 77(14), 18043-18065.

Yange, T. S., Onyekwere, O., & Okeke, O. B. (2020). A Duty Scheduler for Veterinary Teaching Hospitals Using Tabu Search Algorithm. Journal of Computer Sciences and Applications, 8(1), 30-39.

Younis, M. I., Fadhil, H. M., & Jawad, Z. N. (2016). Acceleration of the RSA Processes based on Parallel Decomposition and Chinese Reminder Theorem [J]. International Journal of Application or Innovation in Engineering & Management, 5(1), 12-23.

Yu, C. (2016). Steganography of Digital Watermark Based on Artificial Neural Networks in Image Communication and Intellectual Property Protection. Neural Processing Letters, 44(2), 307-316.

Zainuddin, F. A., & Abd Samad, M. F. (2021). Comparison of Crossover in Genetic Algorithm for Discrete-Time System Identification.

Zainuddin, F. A., & Abd Samad, M. F., (2020). A review of crossover methods and problem representation of genetic algorithm in recent engineering applications. International Journal of Advanced Science and Technology, 29, 759-69.

Zamani, M., Taherdoost, H., Manaf, A. A., Ahmad, R. B., & Zeki, A. M. (2009). Robust audio steganography via genetic algorithm. In 2009 International Conference on Information and Communication Technologies (pp. 149-153). IEEE.

Zeeshan, M., Ullah, S., Anayat, S., Hussain, R. G., & Nasir, N. (2017). A review study on unique way of information hiding: Steganography. International Journal on Data Science and Technology, 3(5), 45-51.

Zeki, A. M., & Manaf, A. A. (2009). A novel digital watermarking technique based on ISB (Intermediate Significant Bit). World Academy of Science, Engineering and Technology, 50, 989-996.

Zeki, A., Abubakar, A., & Chiroma, H. (2016). An intermediate significant bit (ISB) watermarking technique using neural networks. SpringerPlus, 5(1), 868.

Zhou, X., Gong, W., Fu, W., & Jin, L. (2016). An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS) (pp. 1-4). IEEE.

Ziedan, R. H., Mead, M. A., & Eltawel, G. S. (2016). Selecting the Appropriate Feature Extraction Techniques for Automatic Medical Images Classification. International Journal, 1.

Zong, T., Xiang, Y., Natgunanathan, I., Guo, S., Zhou, W., & Beliakov, G. (2014). Robust histogram shape-based method for image watermarking. IEEE Transactions on Circuits and Systems for Video Technology, 25(5), 717-729.

Rodrigues, J. M., Rios, J. R., & Puech, W. (2004, April). SSB-4 System of Steganography using bit 4. In WIAMIS: Workshop on Image Analysis for Multimedia Interactive Services.

Brie, A. H. & Morignot, P. (2005, June). Genetic Planning Using Variable Length Chromosomes. In ICAPS (pp. 320-329).

Fard, A. M., Akbarzadeh-T, M. R., & Varasteh-A, F. (2006, April). A new genetic algorithm approach for secure JPEG steganography. In 2006 IEEE International Conference on Engineering of Intelligent Systems (pp. 1-6). IEEE.

Manoharan, S. (2008, June). An empirical analysis of RS steganalysis. In 2008 The Third International Conference on Internet Monitoring and Protection (pp. 172-177). IEEE.

Khodaei, M., & Faez, K. (2010, June). Image hiding by using genetic algorithm and LSB substitution. In International Conference on Image and Signal Processing (pp. 404-411). Springer, Berlin, Heidelberg.

Bajaj, R., Bedi, P., & Pal, S. K. (2010, December). Best hiding capacity scheme for variable length messages using particle swarm optimization. In International Conference on Swarm, Evolutionary, and Memetic Computing (pp. 230-237). Springer, Berlin, Heidelberg.

Bamatraf, A., Ibrahim, R., & Salleh, M. N. B. M. (2010, December). Digital watermarking algorithm using LSB. In 2010 International Conference on Computer Applications and Industrial Electronics (pp. 155-159). IEEE.

Ghasemi, E., & Shanbehzadeh, J. (2010, December). An imperceptible steganographic method based on Genetic Algorithm. In 2010 5th International Symposium on Telecommunications (pp. 836-839). IEEE.

Ghasemi, E., Shanbehzadeh, J., & Fassihi, N. (2011, March). High capacity image steganography using Wavelet transform and genetic algorithm. In World Congress on Engineering 2012. July 4-6, 2012. London, UK. (Vol. 2188, pp. 495-498). International Association of Engineers.

Bedi, P., Bansal, R., & Sehgal, P. (2011, July). Using PSO in image hiding scheme based on LSB substitution. In International Conference on Advances in Computing and Communications (pp. 259-268). Springer, Berlin, Heidelberg.

Al-Ataby, A. A., & Al-Naima, F. M. (2011, December). High capacity image steganography based on curvelet transform. In 2011 Developments in E-systems Engineering (pp. 191-196). IEEE.

Swain, G., & Lenka, S. K. (2012, December). LSB array based image steganography technique by exploring the four least significant bits. In International Conference

on Computing and Communication Systems (pp. 479-488). Springer, Berlin, Heidelberg.

Deif, D. S. & Gadallah, Y. (2014, April). Wireless sensor network deployment using a variable-length genetic algorithm. In 2014 IEEE wireless communications and networking conference (WCNC) (pp. 2450-2455). IEEE.

Nosrati, M., Hanani, A., & Karimi, R. (2015, February). Steganography in image segments using genetic algorithm. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp. 102-107). IEEE.

Kaswan, K. S., Choudhary, S., & Sharma, K. (2015, March). Applications of artificial bee colony optimization technique: Survey. In 2015 2nd International Conference on Computing for Sustainable Global Development (Indiacom) (pp. 1660-1664). IEEE.

Kaur, S., & Goel, N. (2015, December). Segmentation and block based image steganography using optimal pixel adjustment process and identical approach. In 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS) (pp. 1-5). IEEE.

Johri, P., Mishra, A., Das, S., & Kumar, A. (2016, March). Survey on steganography methods (text, image, audio, video, protocol and network steganography). In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 2906-2909). IEEE.

Kalaiselvi, K., & Kumar, A. (2016, March). Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box. In 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC) (pp. 1-6). IEEE.

Yushkevich, P. A., Gao, Y., & Gerig, G. (2016, August). ITK-SNAP: An interactive tool for semi-automatic segmentation of multi-modality biomedical images. In 2016 38th annual international conference of the IEEE engineering in medicine and biology society (EMBC) (pp. 3342-3345). IEEE.

Khamrui, A., Gupta, D. D., Ghosh, S., & Nandy, S. (2017, March). A Spatial Domain Image Authentication Technique Using Genetic Algorithm. In International Conference on Computational Intelligence, Communications, and Business Analytics (pp. 577-584). Springer, Singapore.

Khamrui, A., Gupta, D. D., Ghosh, S., & Nandy, S. (2017, March). A Spatial Domain Image Authentication Technique Using Genetic Algorithm. In International Conference on Computational Intelligence, Communications, and Business Analytics (pp. 577-584). Springer, Singapore.

Abdel-Nabi, H., & Al-Haj, A. (2017, April). Efficient joint encryption and data hiding algorithm for medical images security. In 2017 8th international conference on information and communication systems (ICICS) (pp. 147-152). IEEE.

Sreekutty, M. S., & Baiju, P. S. (2017, April). Security enhancement in image steganography for medical integrity verification system. In 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-5). IEEE.

Bharti, J., Solanki, S., & Beliya, A. (2017, October). Comparison of LSB methods and pattern. In 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE) (pp. 250-256). IEEE.

Douiri, S. M., & Elbernoussi, S. (2017, October). A Steganographic Method Using Tabu Search Approach. In 2017 Sixteenth Mexican International Conference on Artificial Intelligence (MICAI) (pp. 30-33). IEEE.

Jain, M., & Kumar, A. (2017, December). Secure medical communication using sixteen rectangle substitution cipher and information-location dependent steganography. In 2017 International Conference on Intelligent Communication and Computational Techniques (ICCT) (pp. 189-193). IEEE.

Madoš, B., Balaz, A., Adám, N., & Hurtuk, J. (2018, May). Information hiding into OBJ format file using vector steganography techniques. In 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 00091-00096). IEEE.

Mewalal, N., & Leung, W. S. (2018, June). Improving hidden message extraction using LSB steganalysis techniques. In International Conference on Information Science and Applications (pp. 273-284). Springer, Singapore.

Allaf, A. H., & Kbir, M. A. (2018, October). A review of digital watermarking applications for medical image exchange security. In The proceedings of the third international conference on smart city applications (pp. 472-480). Springer, Cham.

Shah, P. D., & Bichkar, R. S. (2020, June). Genetic Algorithm based Approach to Select Suitable Cover Image for Image Steganography. In 2020 International Conference for Emerging Technology (INCET) (pp. 1-5). IEEE.

Aliefa, M. H., & Suyanto, S. (2020, August). Variable-Length Chromosome for Optimizing the Structure of Recurrent Neural Network. In 2020 International Conference on Data Science and Its Applications (ICoDSA) (pp. 1-5). IEEE.

Sahoo, S., & Sahoo, S. S. (2020, December). A new COVID-19 medical image steganography based on dual encrypted data insertion into minimum mean intensity window of LSB of X-ray scans. In 2020 IEEE 17th India council international conference (INDICON) (pp. 1-6). IEEE.