The copyright © of this thesis belongs to its rightful author and/or other copyright owner. Copies can be accessed and downloaded for non-commercial or learning purposes without any charge and permission. The thesis cannot be reproduced or quoted as a whole without the permission from its rightful owner. No alteration or changes in format is allowed without permission from its rightful owner.

ENHANCING THE ARB-SYLLABLE TECHNIQUE THROUGH MAPPING MECHANISM IN TEXT-BASED STEGANOGRAPHY

FARAH QASIM AHMED ALYOUSUF

Universiti Utara Malaysia

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2025

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)

FARAH QASIM AHMED AL-YOUSUF

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):

"ENHANCING THE ARB-SYLLABLE TECHNIQUE THROUGH MAPPING MECHANISM IN TEXT-BASED STEGANOGRAPHY"

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 : ***20 Mac 2024.***
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: ***20 March 2024.***

Pengerusi Viva: *(Chairman for VIVA)*	**Prof. Dr. Azman Yasin**	Tandatangan *(Signature)*
Pemeriksa Luar: *(External Examiner)*	**Prof. Ts. Dr. Ainuddin Wahid Abdul Wahab**	Tandatangan *(Signature)*
Pemeriksa Dalam: *(Internal Examiner)*	**Assoc. Prof. Dr. Nur Haryani Zakaria**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Assoc. Prof. Dr. Roshidi Din**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Dr. Mohd Saiful Adli Mohamad**	Tandatangan *(Signature)*

Tarikh:
(Date) ***20 March 2024***

Permission to Use

In presenting this thesis in fulfilment 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 Salleh Graduate School of Arts and Sciences. 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 Universiti Utara Malaysia for any scholarly use which may be made of any material from my 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:

Universiti Utara Malaysia

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Ramai penyelidik telah memperkenalkan pelbagai pendekatan steganografi berasaskan teks bagi memastikan data rahsia kekal tidak dapat dikesan. Kaedah rawak dan statistik merupakan antara pendekatan yang menonjol dalam steganografi berasaskan teks, yang melibatkan penyembunyian teks mengikut pengelasan aksara dalam teks perlindungan. Teknik-teknik sedia ada dalam kaedah ini termasuklah Garis Lurus Menegak (VERT), Perubahan Corak Huruf Abjad (CALP), dan Pengkategorian Kuadruple (QUAD). Walau bagaimanapun, kaedah rawak dan statistik menghadapi masalah dalam proses penyisipan berkaitan dengan kapasiti penyembunyian, keselamatan, ketahanan dan prestasi ketidakterlihatan. Oleh itu, kajian ini mencadangkan satu mekanisme pemetaan dalam teknik Arb-Syllable bagi menambah baik kaedah rawak dan statistik yang bergantung kepada transliterasi aksara Arab ke dalam bahasa Inggeris. Kajian ini bertujuan mereka bentuk dan merumuskan mekanisme pemetaan dalam teknik Arb-Syllable untuk pendekatan steganografi berasaskan teks serta menilai prestasinya berbanding teknik-teknik sedia ada. Metodologi yang digunakan melibatkan pembangunan satu teknik yang mengkategorikan aksara Inggeris berdasarkan transliterasi Arab, khususnya sama ada aksara Arab yang sepadan mengandungi titik atau tidak. Hasil eksperimen menunjukkan penambahbaikan yang ketara dalam semua metrik prestasi. Teknik mekanisme pemetaan yang dicadangkan mencapai kadar keselamatan dan ketidakterlihatan sebanyak 100% (Jarak Jaro-Winkler sebanyak 1), berbanding maksimum masing-masing sebanyak 99.99% dan 0.9982 dalam teknik sedia ada. Selain itu, prestasi kapasiti penyembunyian turut meningkat sebanyak 30% berbanding teknik VERT, CALP dan QUAD. Sementara itu, teknik pemetaan yang dicadangkan menunjukkan ketahanan yang lebih tinggi terhadap serangan struktur, dengan mengekalkan integriti mesej tersembunyi apabila berlaku perubahan pemformatan. Kajian ini menyumbang pendekatan yang lebih baik untuk steganografi berasaskan teks dengan mengimbangi kapasiti penyembunyian yang tinggi, keselamatan maksimum dan ketidakterlihatan, sekali gus menangani pertukaran asas dalam sistem steganografi.

Kata Kunci: Steganografi berasaskan teks, Teknik steganografi, Mekanisme pemetaan, Teknik Arb-Syllable, Transliterasi Arab, Metrik prestasi

Abstract

Many researchers have introduced diverse text-based steganography approaches to ensure that secret data remains undetectable. Random and statistical methods are one of the prominent methods used in text-based steganography approaches, involving hiding text according to classified characters in cover text. The existing techniques in this method are Vertical Straight Line (VERT), Changing in Alphabet Letter Patterns (CALP), and Quadruple Categorization (QUAD) techniques. However, random and statistical methods face issues in the embedding process, particularly in terms of hiding capacity, security, robustness, and imperceptibility. Therefore, this study proposes a mapping mechanism that improves the existing techniques in random and statistical method, relying on the transliteration of Arabic characters into the English language. The methodology involved developing a technique that categorizes English characters based on their Arabic transliteration, specifically whether the corresponding Arabic characters contain pointed or un-pointed letters. Experimental results demonstrated significant improvements across all performance metrics (hiding capacity, security, robustness, and imperceptibility). The proposed mapping mechanism technique achieved 100% of security ratio and imperceptibility (Jaro-Winkler distance of 1) rate, compared to maximums of 99.99% and 0.9982 for the VERT, CALP, and QUAD techniques, respectively. Additionally, hiding capacity performance is increased by 30% compared to the VERT, CALP, and QUAD techniques. Meanwhile, the proposed mapping mechanism technique demonstrated higher robustness against structural attacks, preserving the integrity of hidden messages when subjected to formatting changes. This study contributes a better approach to text-based steganography approach that balances high hiding capacity with maximum security and imperceptibility, addressing a fundamental trade-off in steganographic systems.

Keywords: Text-based steganography, Steganography techniques, Mapping mechanism, Arb-Syllable technique, Arabic transliterate, Performances metrics

Acknowledgment

In the name of Allah, the most Gracious and Most Merciful, all the praises are due to Allah (SWT), the Creator, the Sustainer of the universe, and blessings and salutation be upon Prophet Muhammed, His Messenger. I am very grateful to Almighty Allah for the prayers, guidance, strength, and health He bestowed on me during this study period. Without his mercy, it would have been impossible to complete my thesis. I wish to express my sincere gratitude to my supervisors, Assoc. Prof. Dr. Roshidi Bin Din, and Dr. Mohd Saiful Adli Mohamad, for their support, guidance, time, and spirit in making a dream come true. I gained valuable knowledge and experience with them, and I feel honored and grateful to work under their supervision. I would also like to express my sincere gratitude to my beloved family, starting with my Husband, Dr. Firas, and my lovely kids, Fadi and Fahad, my brother Mohammed, and my father and mother, for their Dua and prayers. Mercy and eternity to my older sister (Zina). Unfortunately, she passed away before reaching this level in my PhD journey. Finally, I would like to express my sincere gratitude to all my colleagues at the University Utara Malaysia, who have also contributed to my success and support.

Universiti Utara Malaysia

Table of Contents

Universiti Utara Malaysia

Universiti Utara Malaysia

List of Tables

Universiti Utara Malaysia

List of Figures

Universiti Utara Malaysia

List of Algorithms

Universiti Utara Malaysia

List of Abbreviations

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
CALP	Changing in Alphabet Letter Patterns
coverTxt	Cover Text
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DT-CWT	Dual-Tree Complex Wavelet Transform
DWT	Discrete Wavelet Transform
IDEA	International Data Encryption Algorithm
IWT	Integer Wavelet Transform
LSB	Least Significant Bit
LZW	Lempel–Ziv– Welch
MixColumn	Mix Column
NIST	National Institute Standard and Technology
PVD	Pixel Value Differencing
QUAD	Quadruple Categorization
RC4	Rivest Cipher 4
RC6	Rivest Cipher 6
RoundKey	Add Round Key
scrtMsg	Secret Message
ShiftRow	Shift Row
SMS	Short Message Service
SubByte	Substitute Bytes
VERT	Vertical Strait Line
ZWJ	Zero-Width Joiner
ZWNJ	Zero-Width Non-Joiner

Universiti Utara Malaysia

CHAPTER ONE
INTRODUCTION

1.1 Background of Study

Generally, watermarking, steganography, and cryptography are identified as secured data domains in data protection (Baawi et al., 2018; Bhandari & Kirubanand, 2019). It has been discovered and used widely by many researchers to protect against malicious. Also, it is a barrier to attacks by providing tools and means to protect information from internal or external risks in a data-secured environment (Abood et al., 2022; Alkhudaydi & Gutub, 2020). The watermarking field is used to classify and shield the content of the copyrighted media by hiding the data into the main content, such as e-commerce, smart cities, and e-healthcare applications (Hurrah et al., 2019; Kowalczuk & Holub, 2021; Mun et al., 2019; Wan et al., 2022).

Another field used in secured data is cryptography, as defined by the National Institute Standard and Technology (NIST) in 1977, "uses mathematical techniques to transform data and prevent it from being read or tampered with by unauthorized parties", which is the way that converts any message into an unknown symbol by using specific algorithms to become unreadable and not understandable by unauthorized users. Therefore, authorized people can convert the symbols to the original form by using a unique key (Liu et al., 2016; Nabben, 2023) so that confidentiality of the data will be provided, and it uses the encryption-decryption strategy to secure information (Altigani & Naserelden, 2018).

Meanwhile, the steganography field aims to protect information by a cover and to hide the data in a digital or a text medium and remove the suspects of the existence of secret

REFERENCES

Abood, E. W., Abdullah, A. M., Sibahee, M. A. Al, Ameen, Z., Nyangaresi, V. O., Ahmad, S., Kalafy, A., Jalil, M., & Ghrabta, J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 185–194. https://doi.org/10.11591/eei.v11i1.3279

Abuadbba, A., & Khalil, I. (2015). Wavelet based steganographic technique to protect household confidential information and seal the transmitted smart grid readings. *Information Systems*, *53*, 224–236. https://doi.org/10.1016/j.is.2014.09.004

Acharjee, T., Konwar, A., Ram, R. K., Sharma, R., & Goswami, D. (2016). XORSTEG: A new model of text steganography. *2016 International Conference on Communication and Electronics Systems (ICCES)*, *10*(3), 1–4. https://doi.org/10.1109/CESYS.2016.7889820

Advani, N., Rathod, C., & Gonsai, A. M. (2019). Comparative Study of Various Cryptographic Algorithms Used for Text, Image, and Video. *Advances in Intelligent Systems and Computing*, *841*, 393–399. https://doi.org/10.1007/978-981-13-2285-3_46

Agarwal, M. (2013). Text Steganographic Approaches: A Comparison. *International Journal of Network Security & Its Applications*, *5*(1), 91–106.

Ahvanooey, M. T., Li, Q., Hou, J., Rajput, A. R., & Chen, Y. (2019a). Modern text hiding, text steganalysis, and applications: A comparative analysis. *Entropy*, *21*(4), 1–29. https://doi.org/10.3390/e21040355

Ahvanooey, M. T., Li, Q., Hou, J., Rajput, A. R., & Chen, Y. (2019b). Modern text hiding, text steganalysis, and applications: A comparative analysis. *Entropy*, *21*(4). https://doi.org/10.3390/e21040355

Akotoye, F. X. K., Yakavor, Y. E., Kwofie, J., & Tirogo, F. La. (2018). Character pair text steganography based on the enhanced. *IEEE International Conference on Adaptive Science and Technology, ICAST*, *2018-Augus*, 1–5. https://doi.org/10.1109/ICASTECH.2018.8507117

AL-Hagree, S., Hadwan, M., Aqlan, A., Albazel, M., Alqasemi, F., & Al-Sanabani,

Universiti Utara Malaysia

M. (2021). A Survey on Different Arabic Text Steganography Techniques. *2021 1st International Conference on Emerging Smart Technologies and Applications (ESmarTA)*, 1–8. https://doi.org/10.1109/eSmarTA52612.2021.9515740

Al-Nofaie, S., Gutub, A., & Al-Ghamdi, M. (2021). Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces. *Journal of King Saud University - Computer and Information Sciences*, *33*(8), 963–974. https://doi.org/10.1016/j.jksuci.2019.06.010

Al-Nofaie, S. M. A., & Gutub, A. A. A. (2019). Utilizing pseudo-spaces to improve Arabic text steganography for multimedia data communications. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-019-08025-x

Alanazi, N., Khan, E., & Gutub, A. (2021). Efficient security and capacity techniques for Arabic text steganography via engaging Unicode standard encoding. *Multimedia Tools and Applications*, *80*(1), 1403–1431. https://doi.org/10.1007/s11042-020-09667-y

Alanazi, N., Khan, E., & Gutub, A. (2022). Inclusion of Unicode Standard seamless characters to expand Arabic text steganography for secure individual uses. *Journal of King Saud University - Computer and Information Sciences*, *34*(4), 1343–1356. https://doi.org/10.1016/j.jksuci.2020.04.011

Alghamdi, N., & Berriche, L. (2019). Capacity investigation of Markov chain-based statistical text steganography: Arabic language case. *ACM International Conference Proceeding Series*, 37–43. https://doi.org/10.1145/3314527.3314532

Ali, R. H., & Kadhim, J. M. (2021). Text-based Steganography using Huffman Compression and AES Encryption Algorithm. *Iraqi Journal of Science*, *62*(11), 4110–4120. https://doi.org/10.24996/ijs.2021.62.11.31

Ali Shah, S. T., Khan, D. A., & Hussain, D. A. (2020). Text Steganography Using character Spacing after Normalization. *International Journal of Scientific & Engineering Research*, *11*(2), 949–957. https://doi.org/10.14299/ijser.2020.02.05

Alifah Roslan, N., Izura Udzir, N., Mahmod, R., & Gutub, A. (2022). Systematic literature review and analysis for Arabic text steganography method practically. *Egyptian Informatics Journal*, *23*(4), 177–191.

https://doi.org/10.1016/j.eij.2022.10.003

Alkhudaydi, M. G., & Gutub, A. A. (2020). Integrating Light-Weight Cryptography with Diacritics Arabic Text Steganography Improved for Practical Security Applications. *Journal of Information Security and Cybercrimes Research*, *3*(1), 13–30. https://doi.org/10.26735/fmit1649

Alkhudaydi, M., & Gutub, A. (2021). Securing Data via Cryptography and Arabic Text Steganography. *SN Computer Science*, *2*(1), 1–18. https://doi.org/10.1007/s42979-020-00438-y

Almehmadi, E., & Gutub, A. (2022). Novel Arabic e-Text Watermarking Supporting Partial Dishonesty Based on Counting-Based Secret Sharing. *Arabian Journal for Science and Engineering*, *47*(2), 2585–2609. https://doi.org/10.1007/s13369-021-06200-7

Alqahtany, S. S., Alkhodre, A. B., Al Abdulwahid, A., & Alohaly, M. (2023). A Dynamic Multi-Layer Steganography Approach Based on Arabic Letters' Diacritics and Image Layers. *Applied Sciences*, *13*(12), 7294. https://doi.org/10.3390/app13127294

Alshamsi, A., Albaloushi, S., Alkhoori, M., Almheiri, H., & Ababneh, N. (2022). Enhancing Arabic Text Steganography Based on Unicode Features. *International Journal of Computing and Digital Systems*, *11*(1), 685–693. https://doi.org/10.12785/ijcds/110155

Altigani, A., & Barry, B. (2013). A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and Word Shift Coding Protocol. *Proceedings - 2013 International Conference on Computer, Electrical and Electronics Engineering: "Research Makes a Difference", ICCEEE 2013*, 134–139. https://doi.org/10.1109/ICCEEE.2013.6633920

Altigani, A., & Naserelden, S. (2018). Optimized hybrid approach to secure transmitted messages using the advanced encryption standard and the word shift coding protocol. *Journal of Theoretical and Applied Information Technology*, *96*(17), 5740–5750.

Askari, M., Mahmood, A., & Iqbal, Z. (2023). A novel font color and compression text steganography technique. *2023 International Conference on*

Communication, Computing and Digital Systems (C-CODE), 1–6. https://doi.org/10.1109/C-CODE58145.2023.10139867

Azeem, M., He, J., Rana, K. G., & Akhtar, F. (2019). A cryptographic data hiding algorithm with high cover text capacity. *International Journal of Electronic Security and Digital Forensics*, *11*(2), 225. https://doi.org/10.1504/IJESDF.2019.098804

Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2017). New text steganography technique based on a set of two-letter words. *Journal of Theoretical and Applied Information Technology*, *95*(22), 6247–6255.

Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2018). A comparative study on the advancement of text steganography techniques in digital media. *ARPN Journal of Engineering and Applied Sciences*, *13*(5), 1854–1863.

Baawi, S. S., Mokhtar, M. R., & Sulaiman, R. (2019). *Enhancement of Text Steganography Technique Using Lempel-Ziv-Welch Algorithm and Two-Letter Word Technique* (Vol. 843, pp. 525–537). Springer International Publishing. https://doi.org/10.1007/978-3-319-99007-1_49

Barani, M. J., Valandar, M. Y., & Ayubi, P. (2019). A new digital image tamper detection algorithm based on integer wavelet transform and secured by encrypted authentication sequence with 3D quantum map. *Optik - International Journal for Light and Electron Optics 187*, *187*(November 2018), 205–222. https://doi.org/10.1016/j.ijleo.2019.04.074

Bensaad, M. L., & Yagoubi, M. B. (2011). High capacity diacritics-based method for information hiding in Arabic text. *2011 International Conference on Innovations in Information Technology, IIT 2011*, 433–436. https://doi.org/10.1109/INNOVATIONS.2011.5893864

Bensaad, M. L., & Yagoubi, M. B. (2013). Boosting the Capacity of Diacritics-Based Methods for Information Hiding in Arabic Text. *Arabian Journal for Science and Engineering*, *38*(8), 2035–2041. https://doi.org/10.1007/s13369-013-0576-3

Bhandari, R., & Kirubanand, V. B. (2019). Enhanced encryption technique for secure iot data transmission. *International Journal of Electrical and Computer Engineering (IJECE)*, *9*(5), 3732–3738.

Universiti Utara Malaysia

https://doi.org/10.11591/ijece.v9i5.pp3732-3738

Bhanot, R., & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications*, *9*(4), 289–306. https://doi.org/10.14257/ijsia.2015.9.4.27

Bhat, D., Krithi, V., Manjunath, K. N., Prabhu, S., & Renuka, A. (2017). Information hiding through dynamic text steganography and cryptography: Computing and Informatics. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, *2017-Janua*, 1826–1831. https://doi.org/10.1109/ICACCI.2017.8126110

Bhattacharyya, S., Indu, P., Dutta, S., Biswas, A., & Sanyal, G. (2011). Hiding Data in Text Through Changing in Alphabet Letter Patterns (CALP). *Journal of Global Research in Computer Science*, *2*(3), 33–39.

Bhaya, W., Rahma, A. M., & AL-Nasrawi, D. (2013). Text steganography based on font type in MS-word documents. *Journal of Computer Science*, *9*(7), 898–904. https://doi.org/10.3844/jcssp.2013.898.904

Chandel, B., & Jain, S. (2016). *Video Steganography : A Survey*. *18*(1), 11–17. https://doi.org/10.9790/0661-18131117

Chaudhary, S., Dave, M., & Sanghi, A. (2016). Text steganography based on feature coding method. *ACM International Conference Proceeding Series*, *12-13-Augu*, 5–8. https://doi.org/10.1145/2979779.2979786

Chaudhary, S., Dave, M., & Sanghi, A. (2017). Aggrandize text security and hiding data through text steganography. *2016 IEEE 7th Power India International Conference, PIICON 2016*, 1–5. https://doi.org/10.1109/POWERI.2016.8077346

Chaudhary, S., Dave, M., Sanghi, A., & Sidh, H. (2018). Indian Script Encoding Technique (ISET): A Hindi Text Steganography Approach. In *Lecture Notes in Networks and Systems* (Vol. 9, pp. 393–401). https://doi.org/10.1007/978-981-10-3932-4_41

Ciptaningtyas, H. T., Anggoro, R., & Fadhillah, M. B. A. (2018). Text Steganography on Sundanese Script using Improved Line Shift Coding. *2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-*

Universiti Utara Malaysia

KCIC), 254–261. https://doi.org/10.1109/KCIC.2018.8628471

Daggumati, G. P., & Banik, B. G. (2022). Comprehensive study of video steganography using convolutional neural networks using temporal redundancy. *AIP Conference Proceedings*, *2640*, 110085. https://doi.org/10.1063/5.0110085

Darbani, A., Alyannezhadi, M. M., & Forghani, M. (2019). A New Steganography Method for Embedding Message in JPEG Images. *2019 IEEE 5th Conference on Knowledge Based Engineering and Innovation, KBEI 2019*, 617–621. https://doi.org/10.1109/KBEI.2019.8735054

Das, P., Munshi, N. H., & Maitra, S. (2021). New Key-Dependent S-Box Generation Algorithm on AES. *Micro and Nanosystems*, *14*(3), 263–271. https://doi.org/10.2174/1876402913666210726163822

Davila, J. (1999). Genetic optimization of NN topologies for the task of natural language processing. *Proceedings of the International Joint Conference on Neural Networks*, *2*(April), 821–826. https://doi.org/10.1109/ijcnn.1999.831057

Dey, A. K., Behera, G. G., & Mishra, A. K. (2024). *An English Sentence Dictionary Based Secure Text Steganographic Technique for Message-Data Confidentiality BT - Computing, Communication and Learning* (S. K. Panda, R. R. Rout, M. Bisi, R. C. Sadam, K.-C. Li, & V. Piuri (eds.); pp. 297–307). Springer Nature Switzerland.

Din, R., Bakar, R., Utama, S., Jasmis, J., & Elias, S. J. (2019). The evaluation performance of letter-based technique on text steganography system. *Bulletin of Electrical Engineering and Informatics*, *8*(1), 291–297. https://doi.org/10.11591/eei.v8i1.1440

Din, R., & Utama, S. (2017). Critical Review of Verification and Validation Process in Feature-Based Method Steganography. *International Conference on E-Commerce*, 15–19.

Din, R., Utama, S., Hanizan, S. H., Hilal, M. M., Hanif, M. A. M., Zulhazlin, A., & Fazali, G. M. (2018). Evaluating the Feature-Based Technique of Text Steganography Based on Capacity and Time Processing Parameters. *Advanced Science Letters*, *24*(10), 7355–7359. https://doi.org/10.1166/asl.2018.12941

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. https://doi.org/10.11591/ijeecs.v11.i2.pp747-754

Ding, C., Fu, Z., Yu, Q., Wang, F., & Chen, X. (2023). Joint Linguistic Steganography With BERT Masked Language Model and Graph Attention Network. *IEEE Transactions on Cognitive and Developmental Systems*, 3296413. https://doi.org/10.1109/TCDS.2023.3296413

Ditta, A., Azeem, M., Naseem, S., Gulzar Rana, K., Adnan Khan, M., & Iqbal, Z. (2022). A secure and size efficient algorithm to enhance data hiding capacity and security of cover text by using unicode. *Journal of King Saud University - Computer and Information Sciences*, *34*(5), 2180–2191. https://doi.org/10.1016/j.jksuci.2020.07.010

Dulera, S., Jinwala, D., & Dasgupta, A. (2011). Experimenting with The Novel Approaches in Text Steganography. *International Journal of Network Security & Its Applications (IJNSA)*, *3*(6).

El-Khamy, S. E., Korany, N. O., & El-Sherif, M. H. (2017). A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption. *Multimedia Tools and Applications*, *76*(22), 24091–24106. https://doi.org/10.1007/s11042-016-4113-8

El Rahman, S. A. (2019). Text steganography approaches using similarity of English font styles. *International Journal of Software Innovation*, *7*(3), 29–50. https://doi.org/10.4018/IJSI.2019070102

Farhan, A. K., Ali, R. S., & Ali, S. M. (2019). Secure Location Map and Encryption Key Based on Intelligence Search Algorithm in Encryption and Steganography to Data Protection. *International Journal of Mechanical Engineering and Technology*, *10*(1), 8–24. http://www.iaeme.com/IJMET/index.asp8http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=10&IType=1http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=10&IType=1

Goyal, H., & Bansal, P. (2015). An Analytical Study on Video Steganography Techniques. *International Journal of Advanced Research in Computer Science*,

6(5), 50–52.

Gunawan, A., Richard, Susanto, G. A., Saputra, A., & Rizal, A. C. (2022). Understanding the Use of Blockchain in Medical Data Security: A Systematic Literature Review. *ACM International Conference Proceeding Series*, 170–174. https://doi.org/10.1145/3581971.3581995

Gupta Banik, B., & Bandyopadhyay, S. K. (2020). Novel Text Steganography Using Natural Language Processing and Part-of-Speech Tagging. *IETE Journal of Research*, *66*(3), 384–395. https://doi.org/10.1080/03772063.2018.1491807

Gutub, A. A.-A., & Alaseri, K. A. (2021). Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing. *Journal of King Saud University - Computer and Information Sciences*, *33*(9), 1108–1120. https://doi.org/10.1016/j.jksuci.2019.06.014

Gutub, A., & Alaseri, K. (2019). Hiding Shares of Counting-Based Secret Sharing via Arabic Text Steganography for Personal Usage. *Arabian Journal for Science and Engineering*, *0123456789*. https://doi.org/10.1007/s13369-019-04010-6

Hashim, J., Hameed, A., Abbas, M. J., Awais, M., Qazi, H. A., & Abbas, S. (2018). LSB Modification based Audio Steganography using Advanced Encryption Standard (AES-256) Technique. *2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 1–6. https://doi.org/10.1109/MACS.2018.8628458

Hurrah, N. N., Parah, S. A., Loan, N. A., Sheikh, J. A., Elhoseny, M., & Muhammad, K. (2019). Dual watermarking framework for privacy protection and content authentication of multimedia. *Future Generation Computer Systems*, *94*, 654–673. https://doi.org/10.1016/j.future.2018.12.036

Iyer, S. S., & Lakhtaria, K. (2016). New robust and secure alphabet pairing Text Steganography Algorithm. *International Journal of Current Trends in Engineering & Research (IJCTER)*, *2*(7), 15–21.

Iyer, S. S., & Lakhtaria, K. (2017). Practical Evaluation and Comparative Study of Text Steganography Algorithms. *International Journal of Advance Engineering and Research*, *3*(4).

Jeevitha, S., & Amutha Prabha, N. (2018). A comprehensive review on steganographic

techniques and implementation. *ARPN Journal of Engineering and Applied Sciences*, *13*(17), 4780–4791.

Jusoh, S., Mustapha, A., Ismail, A., & Din, R. (2020). A review of Arabic text steganography: Past and present. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(2), 1040–1046. https://doi.org/10.11591/ijeecs.v17.i2.pp1040-1046

Kadhem, S. M. (2016). *Text Steganography Method Based On Modified Run Length Encoding*. *57*(3), 2338–2347.

Kadhim, I. J., Premaratne, P., & Vial, P. J. (2018). Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform. In *Huang DS., Gromiha M., Han K., Hussain A. (eds) Intelligent Computing Methodologies. ICIC 2018. Lecture Notes in Computer Science* (Vol. 10956, pp. 544–550). Springer International Publishing. https://doi.org/10.1007/978-3-319-95957-3_57

Karri, S., & Sur, A. (2015). Steganographic algorithm based on randomization of DCT kernel. *Multimedia Tools and Applications*, *74*(21), 9207–9230. https://doi.org/10.1007/s11042-014-2077-0

Khairullah, M. (2009). A novel text steganography system using font color of the invisible characters in microsoft word documents. *2009 International Conference on Computer and Electrical Engineering, ICCEE 2009*, *1*, 482–484. https://doi.org/10.1109/ICCEE.2009.127

Khairullah, M. (2019). A novel steganography method using transliteration of Bengali text. *Journal of King Saud University - Computer and Information Sciences*, *31*(3), 348–366. https://doi.org/10.1016/j.jksuci.2018.01.008

Khaleel Faieq, A., & Mijwil, M. M. (2022). Prediction of heart diseases utilising support vector machine and artificial neural network. *Indonesian Journal of Electrical Engineering and Computer Science*, *26*(1), 374–380. https://doi.org/10.11591/ijeecs.v26.i1.pp374-380

Khan, A. A., Shaikh, A. A., Cheikhrouhou, O., Laghari, A. A., Rashid, M., Shafiq, M., & Hamam, H. (2022). IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. *IET Image Processing*,

Universiti Utara Malaysia

16(11), 2854–2862. https://doi.org/10.1049/ipr2.12272

Khan, S., Abhijitha, B., Sankineni, R., & Sunil, B. (2015). Polish text steganography method using letter points and extension. *Proceedings of 2015 IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT 2015*, 1–5. https://doi.org/10.1109/ICECCT.2015.7226092

Khan, Y., Algarni, A., Fayomi, A., & Almarashi, A. M. (2021). Disbursal of Text Steganography in the Space of Double-Secure Algorithm. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/7336474

Khekan, A. R., Majeed, H. M. W., & Ahmed Adeeb, O. F. (2021). New text steganography method using the arabic letters dots. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(3), 1784–1793. https://doi.org/10.11591/ijeecs.v21.i3.pp1784-1793

Khosravi, B., Khosravi, B., Khosravi, B., & Nazarkardeh, K. (2019). A new method for pdf steganography in justified texts. *Journal of Information Security and Applications*, *45*, 61–70. https://doi.org/10.1016/j.jisa.2019.01.003

KL, S. N., & R, B. K. (2024). Text steganography: enhanced character-level embedding algorithm using font attribute with increased resilience to statistical attacks. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-19272-y

Kowalczuk, Y., & Holub, J. (2021). Evaluation of digital watermarking on subjective speech quality. *Scientific Reports*, *11*(1). https://doi.org/10.1038/s41598-021-99811-x

Krishnan, R. B., Thandra, P. K., & Baba, M. S. (2017). An overview of text steganography. *2017 4th International Conference on Signal Processing, Communication and Networking, ICSCN 2017*, 0–5. https://doi.org/10.1109/ICSCN.2017.8085643

Kumar, A., & Pooja, K. (2010). Steganography- A Data Hiding Technique. *International Journal of Computer Applications*, *9*(7), 19–23. https://doi.org/10.5120/1398-1887

Kumar, R., Chand, S., & Singh, S. (2014). An Email based high capacity text

Universiti Utara Malaysia

steganography scheme using combinatorial compression. *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*, 336–339. https://doi.org/10.1109/CONFLUENCE.2014.6949231

Kusuma, E. J., Sari, C. A., Rachmawanto, E. H., & Setiadi, D. R. I. M. (2018). A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography. *Journal of ICT Research and Applications*, *12*(2), 103. https://doi.org/10.5614/itbj.ict.res.appl.2018.12.2.1

Lavanya, D., Naresh, G. U. S., Sai, B. B., & Rao, K. P. C. (2023). Quantum Text Steganography By Using BB84 Protocol. *Journal of Engineering Science*, *14*(03), 603–611.

Li, H., Huang, Q., Shen, J., Yang, G., & Susilo, W. (2019). Designated-server identity-based authenticated encryption with keyword search for encrypted emails. *Information Sciences*, *481*, 330–343. https://doi.org/10.1016/j.ins.2019.01.004

Li, L., Huang, L., Zhao, X., Yang, W., & Chen, Z. (2008). A statistical attack on a kind of word-shift text-steganography. *Proceedings - 2008 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2008*, 1503–1507. https://doi.org/10.1109/IIH-MSP.2008.42

Li, S., Wang, J., & Liu, P. (2023). Detection of Generative Linguistic Steganography Based on Explicit and Latent Text Word Relation Mining Using Deep Learning. *IEEE Transactions on Dependable and Secure Computing*, *20*(2), 1476–1487. https://doi.org/10.1109/TDSC.2022.3156972

Lingjun, L., Liusheng, H., Wei, Y., Xinxin, Z., Zhenshan, Y., & Zhili, C. (2008). Detection of word shift steganography in PDF document. *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm'08*, 22–25. https://doi.org/10.1145/1460877.1460897

Liu, Y., Wu, J., & Chen, X. (2021). An Improved Coverless Text Steganography Algorithm Based on Pretreatment and POS. *KSII Transactions on Internet and Information Systems*, *15*(4), 1553–1567. https://doi.org/10.3837/tiis.2020.04.020

Liu, Y., Wu, J., & Xin, G. (2018). Multi-keywords carrier-free text steganography based on part of speech tagging. *ICNC-FSKD 2017 - 13th International*

Universiti Utara Malaysia

Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, 2102–2107. https://doi.org/10.1109/FSKD.2017.8393096

Liu, Y., Yang, T., & Xin, G. (2015). Text steganography in chat based on emoticons and interjections. *Journal of Computational and Theoretical Nanoscience*, *12*(9), 2091–2094. https://doi.org/10.1166/jctn.2015.3992

Liu, Z., Weng, J., Hu, Z., & Seo, H. (2016). Efficient Elliptic Curve Cryptography for Embedded Devices. *ACM Transactions on Embedded Computing Systems*, *16*(2), 1–18. https://doi.org/10.1145/2967103

Luo, Y., & Huang, Y. (2017). Text Steganography with High Embedding Rate. *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 99–104. https://doi.org/10.1145/3082031.3083240

Mabrouk, K. M., Semary, N. A., & Abdul-Kader, H. (2020). Fragile Watermarking Techniques for 3D Model Authentication: Review. In *International Conference on Advanced Machine Learning Technologies and Applications* (pp. 669–679). Springer International Publishing. https://doi.org/10.1007/978-3-030-14118-9_66

Mahato, S., Yadav, D. K., & Khan, D. A. (2013). A Modified Approach to Text Steganography Using HyperText Markup Language. *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, 40–44. https://doi.org/10.1109/ACCT.2013.19

Maitri, P. V., & Verma, A. (2016). Secure file storage in cloud computing using hybrid cryptography algorithm. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, 1635–1638. https://doi.org/10.1109/WiSPNET.2016.7566416

Majeed, M. A., & Sulaiman, R. (2021). A Review on Text Steganography Techniques. *Mathematics*, *9*(21). https://doi.org/10.3390/math9212829

Majeed, M. A., Sulaiman, R., & Shukur, Z. (2022). New Text Steganography Technique based on Multilayer Encoding with Format-Preserving Encryption and Huffman Coding. *International Journal of Advanced Computer Science and Applications*, *13*(12), 163–172. https://doi.org/10.14569/IJACSA.2022.0131222

Majeed, M. A., Sulaiman, R., & Shukur, Z. (2024). New Text Steganography

Universiti Utara Malaysia

Technique Based on Part-of-Speech Tagging and Format-Preserving Encryption. *KSII Transactions on Internet and Information Systems*, *18*(1), 170–191. https://doi.org/10.3837/tiis.2024.01.010

Majercak, D., Banoci, V., Broda, M., Bugar, G., & Levicky, D. (2013). Performance evaluation of feature-based steganalysis in steganography. *Proceedings of 23rd International Conference, RADIOELEKTRONIKA 2013*, 377–382. https://doi.org/10.1109/RadioElek.2013.6530948

Maji, G., & Mandal, S. (2020). A forward email based high capacity text steganography technique using a randomized and indexed word dictionary. *Multimedia Tools and Applications*, *79*(35–36), 26549–26569. https://doi.org/10.1007/s11042-020-09329-z

Majumder, A., & Changder, S. (2013). A Novel Approach for Text Steganography: Generating Text Summary Using Reflection Symmetry. *Procedia Technology*, *10*, 112–120. https://doi.org/10.1016/j.protcy.2013.12.343

Majumder, A., & Changder, S. (2019). A Generalized Model of Text Steganography by Summary Generation using Frequency Analysis. *2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 599–605. https://doi.org/10.1109/icrito.2018.8748747

Majumder, A., Majumdar, A., Podder, T., Kar, N., & Sharma, M. (2015). Secure data communication and cryptography based on DNA based message encoding. *Proceedings of 2014 IEEE International Conference on Advanced Communication, Control and Computing Technologies, ICACCCT 2014*, *978*, 360–363. https://doi.org/10.1109/ICACCCT.2014.7019464

Malalla, S., & Shareef, F. R. (2016). Improving Hiding Security of Arabic Text Steganography by Hybrid AES Cryptography and Text Steganography. *Journal of Engineering Research and Application Www.Ijera.Com ISSN*, *6*(65), 2248–962260. www.ijera.com

Malik, A., Sikka, G., & Verma, H. K. (2017). A high capacity text steganography scheme based on LZW compression and color coding. *Engineering Science and Technology, an International Journal*, *20*(1), 72–79.

https://doi.org/10.1016/j.jestch.2016.06.005

Mandadi, A., Boppana, S., Ravella, V., & Kavitha, R. (2022). Phishing Website Detection Using Machine Learning. *2022 IEEE 7th International Conference for Convergence in Technology, I2CT 2022*, *155*(4), 1140–1145. https://doi.org/10.1109/I2CT54291.2022.9824801

Mandai, K. K., Jana, A., & Agarwal, V. (2014). A new approach of text steganography based on mathematical model of number system. *2014 International Conference on Circuits, Power and Computing Technologies, ICCPCT 2014*, 1737–1741. https://doi.org/10.1109/ICCPCT.2014.7054849

Memon, J., Khowaja, K., & Kazi, H. (2015). Evaluation of Steganography for Urdu / Arabic Text. *Journal of Theoretical and Applied Information Technology*.

Mohamed, A. A. (2014). An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. *Egyptian Informatics Journal*, *15*(2), 79–87. https://doi.org/10.1016/j.eij.2014.04.002

Mohammed, M. H. (2022). Analysis on Contribution of Cryptography and Steganography in Protecting Information in Diverse Environments. *Lecture Notes in Electrical Engineering*, *844*, 153–158. https://doi.org/10.1007/978-981-16-8862-1_11

Monika, A., Eswari, R., & Singh, S. (2023). Detection of Location of Audio-Stegware in LSB Audio Steganography. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 163, pp. 447–459). https://doi.org/10.1007/978-981-99-0609-3_31

Mun, S. M., Nam, S. H., Jang, H., Kim, D., & Lee, H. K. (2019). Finding robust domain from attacks: A learning framework for blind watermarking. *Neurocomputing*, *337*, 191–202. https://doi.org/10.1016/j.neucom.2019.01.067

Nabben, K. (2023). Cryptoeconomics as governance: an intellectual history from "Crypto Anarchy" to "Cryptoeconomics." *Internet Histories*, *0*(0), 1–23. https://doi.org/10.1080/24701475.2023.2183643

Nagare, S., Dapke, P., Quadri, S. A., & Bandal, S. B. (2023). A Review on Various Approaches on Spam Detection of Mobile Phone SMS. *International Journal for Research in Engineering Application & Management (IJREAM)*, *9*(2), 8–11.

Universiti Utara Malaysia

https://doi.org/10.35291/2454-9150.2023.0115

Naharuddin, A., Wibawa, A. D., & Sumpeno, S. (2019). A High Capacity and Imperceptible Text Steganography Using Binary Digit Mapping on ASCII Characters. *Proceeding - 2018 International Seminar on Intelligent Technology and Its Application, ISITIA 2018*, 287–292. https://doi.org/10.1109/ISITIA.2018.8711087

Naqvi, N., Abbasi, A. T., Hussain, R., Khan, M. A., & Ahmad, B. (2018). Multilayer Partially Homomorphic Encryption Text Steganography (MLPHE-TS): A Zero Steganography Approach. *Wireless Personal Communications*, *103*(2), 1563–1585. https://doi.org/10.1007/s11277-018-5868-1

Obeidat, A. A. (2017). Arabic text steganography using Unicode of non-joined to right side letters. *Journal of Computer Science*, *13*(6), 184–191. https://doi.org/10.3844/jcssp.2017.184.191

Odeh, A., Alzubi, A., Hani, Q. B., & Elleithy, K. (2012). Steganography by multipoint Arabic letters. *2012 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–7. https://doi.org/10.1109/LISAT.2012.6223209

Osman, B., Din, R., & Idrus, M. R. (2015). Capacity performance of steganography method in text based domain. *ARPN Journal of Engineering and Applied Sciences*, *10*(3), 1345–1351.

Osman, B., Yahya, N. I., Mohd Zaini, K., & Abdullah, A. (2023). Text Steganography Using the Second Quotient Remainder Theorem and Dark Colour Schemes. *Journal of Computational Innovation and Analytics (JCIA)*, *2*(1), 21–40. https://doi.org/10.32890/jcia2023.2.1.2

Park, Y. H., Park, K. S., & Park, Y. H. (2019). Secure user authentication scheme with novel server mutual verification for multiserver environments. *International Journal of Communication Systems*, *32*(7), 1–17. https://doi.org/10.1002/dac.3929

Peng, J., Sun, Y., Chen, H., Xu, T., Li, Z., Zhang, Q., & Zhang, J. (2019). High-precision and low-complexity symbol synchronization algorithm based on dual-threshold amplitude decision for real-time IMDD OFDM-PON. *IEEE Photonics Journal*, *11*(1), 1–14. https://doi.org/10.1109/JPHOT.2019.2896057

Universiti Utara Malaysia

Peng, J., Zhao, H., Zhao, K., Wang, Z., & Yao, L. (2023). CourtNet: Dynamically balance the precision and recall rates in infrared small target detection. *Expert Systems with Applications*, *233*(May), 120996. https://doi.org/10.1016/j.eswa.2023.120996

Peng, W., Wang, T., Qian, Z., Li, S., & Zhang, X. (2023). Cross-Modal Text Steganography Against Synonym Substitution-Based Text Attack. *IEEE Signal Processing Letters*, *30*(March), 299–303. https://doi.org/10.1109/LSP.2023.3258862

Piotr, J. (2020). *Correspondent Sensitive Encryption Standard (CSES) Algorithm in Insecure Communication Channel*. 90–98.

Prasetyadi, G. C., Mutiara, B. A., & Refianti, R. (2018). File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method. *Proceedings of the 2nd International Conference on Informatics and Computing, ICIC 2017*, *2018-Janua*, 1–5. https://doi.org/10.1109/IAC.2017.8280584

Rahim, T., Khan, S., Usman, M. A., & Shin, S. Y. (2019). Impact of denoising on watermarking: A perspective for information retrieval. *2019 42nd International Conference on Telecommunications and Signal Processing, TSP 2019*, 685–689. https://doi.org/10.1109/TSP.2019.8768896

Rahman, S., Uddin, J., Hussain, H., Jan, S., Khan, I., Shabir, M., & Musa, S. (2023). Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats. *Sustainability (Switzerland)*, *15*(5). https://doi.org/10.3390/su15054252

Rajput, S. P., Adhiya, K. P., & Patnaik, G. K. (2017). An Efficient Audio Steganography Technique to Hide Text in Audio. *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, 1–6. https://doi.org/10.1109/ICCUBEA.2017.8463948

Rangaswamaiah, C., Bai, Y., & Choi, Y. (2020). Multilevel Data Concealing Technique Using Steganography and Visual Cryptography. *Lecture Notes in Networks and Systems*, *70*, 739–758. https://doi.org/10.1007/978-3-030-12385-7

Reddy, I. R. S., & Murali, G. (2017). A novel triple DES to enhance E-governance

Universiti Utara Malaysia

security. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, *August*, 2443–2446. https://doi.org/10.1109/ICECDS.2017.8389889

Roslan, N. A., Mahmod, R., Udzir, N. U. R. I., & Zurkarnain, Z. A. (2014). Primitive Structural Method for High Capacity Text Steganography. *Journal of Theoretical & Applied Information Technology*, *67*(2), 373–383.

Roy, S., & Manasmita, M. (2011). A novel approach to format based text steganography. *Proceedings of the 2011 International Conference on Communication, Computing & Security - ICCCS '11*, 511. https://doi.org/10.1145/1947940.1948046

Roy, S., & Venkateswaran, P. (2013). A Text based Steganography Technique with Indian Root. *Procedia Technology*, *10*, 167–171. https://doi.org/10.1016/j.protcy.2013.12.349

Saad, E., Al, N., & Algamdi, A. (2022). Survey steganography applications. *Al-Salam Journal for Engineering and Technology*, 69–75. https://doi.org/10.55145/ajest.2023.01.01.008

Sabanci, K., u¨nlersen, M. F., & Polat, K. (2016). Classification of different forest types with machine learning algorithms. *Research for Rural Development*, *1*, 254–260.

Sagar, V., Kumar, K., & Vishnoi, V. K. (2019). A Comparative Analysis of Comparative Algorithms. *International Journal of Research and Analytical Reviews (IJRAR)*, *6*(1). https://doi.org/10.1729/Journal.20384

Sahu, N., Peng, D., & Sharif, H. (2017). Unequal steganography with unequal error protection for wireless physiological signal transmission. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2017.7996377

Satir, E., & Isik, H. (2012). A compression-based text steganography method. *Journal of Systems and Software*, *85*(10), 2385–2394. https://doi.org/10.1016/j.jss.2012.05.027

Sharma, M. K., Agarwal, S., & Tech, P. M. (2013). Adaptive Steganographic Algorithm using Cryptographic Encryption RSA Algorithms. *Journal of Engineering, Computers & Applied Sciences*, *2*(1), 2–4.

Universiti Utara Malaysia

Sharma, S., Gupta, A., Trivedi, M. C., & Yadav, V. K. (2016). Analysis of Different Text Steganography Techniques: A Survey. *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, 130–133. https://doi.org/10.1109/CICT.2016.34

Sheshasaayee, A., & Sujatha, D. (2017). Analysis of techniques involving data hiding and watermarking. *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 593–596. https://doi.org/10.1109/ICIMIA.2017.7975529

Shivani, Yadav, V. K., & Batham, S. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. *Procedia Computer Science*, *57*, 1401–1410. https://doi.org/10.1016/j.procs.2015.07.457

Singh, H., Singh, K., & Saroha, K. (2009). A Survey on Text Based Steganography. *Proceedings of the 3rd National Conference; INDIACom-2009*.

Singh, N. (2020). *XOR Encryption Techniques of Video Steganography: A Comparative Analysis* (pp. 203–214). Springer International Publishing. https://doi.org/10.1007/978-3-030-16657-1_19

Sönmez, Y., Tuncer, T., Gökal, H., & Avci, E. (2018). Phishing web sites features classification based on extreme learning machine. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, *2018-Janua*(March), 1–5. https://doi.org/10.1109/ISDFS.2018.8355342

Soualmi, A., Alti, A., Laouamer, L., & Benyoucef, M. (2020). *A Blind Fragile Based Medical Image Authentication Using Schur Decomposition* (Vol. 723, pp. 623–632). Springer International Publishing. https://doi.org/10.1007/978-3-030-14118-9_62

Stojanov, I., Mileva, A., & Stojanovi, I. (2014). A New Property Coding in Text Steganography of Microsoft Word Documents. *8th International Conference on Emerging Security Information, Systems and Technologies*, 25–30.

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering*, *518*, 052003. https://doi.org/10.1088/1757-899x/518/5/052003

Universiti Utara Malaysia

Taleby Ahvanooey, M., Zhu, M. X., Mazurczyk, W., Li, Q., Kilger, M., Choo, K. K. R., & Conti, M. (2022). CovertSYS: A systematic covert communication approach for providing secure end-to-end conversation via social networks. *Journal of Information Security and Applications*, *71*, 103368. https://doi.org/10.1016/j.jisa.2022.103368

Tayyeh, H. K., Mahdi, M. S., & Ahmed AL-Jumaili, A. S. (2019). Novel steganography scheme using Arabic text features in Holy Quran. *International Journal of Electrical and Computer Engineering (IJECE)*, *9*(3), 1910. https://doi.org/10.11591/ijece.v9i3.pp1910-1918

Thabit, R., Udzir, N. I., Md Yasin, S., Asmawi, A., Roslan, N. A., & Din, R. (2021). A comparative analysis of arabic text steganography. *Applied Sciences (Switzerland)*, *11*(15). https://doi.org/10.3390/app11156851

Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., & Gutub, A. A. A. (2022). CSNTSteg: Color Spacing Normalization Text Steganography Model to Improve Capacity and Invisibility of Hidden Data. *IEEE Access*, *10*, 65439–65458. https://doi.org/10.1109/ACCESS.2022.3182712

Tripathi, P. K., Shukla, R. K., Tiwari, N. K., Thakur, B. K., Tripathi, R., & Pal, S. (2022). Enhancing Security of PGP with Steganography. *Proceedings of the 2022 11th International Conference on System Modeling and Advancement in Research Trends, SMART 2022*, 1555–1560. https://doi.org/10.1109/SMART55829.2022.10046709

Tyagi, S., Dwivedi, R., & Saxena, A. (2019). A High Capacity PDF Text Steganography Technique Based on Hashing Using Quadratic Probing. *International Journal of Intelligent Engineering and Systems*, *12*(3), 192–202. https://doi.org/10.22266/ijies2019.0630.20

Utama, S. (2017). DESIGN OF EVALUATION PROCEDURES FOR LETTER-BASED TECHNIQUES IN TEXT STE GANOGRAPHY METHOD SUNARIYA UTAMA MASTER OF SCIENCE (INFORMATION TECHNOLOGY) UNIVERSITI UTARA MALAYSIA. *MASTER OF SCIENCE (INFORMATION TECHNOLOGY) UNIVERSITI UTARA MALAYSIA*. https://linkinghub.elsevier.com/retrieve/pii/S0164121212001379

Universiti Utara Malaysia

Utama, S., & Din, R. (2022). Performance Review of Feature-Based Method in Implementation Text Steganography Approach. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *28*(2), 325–333. https://doi.org/10.37934/araset.28.2.325333

Utama, S., Din, R., & Mahmuddin, M. (2016). Critical analysis on steganography technique in text domain. *Proceedings of the 5th International Cryptology and Information Security Conference 2016, CRYPTOLOGY 2016*, *December*, 150–157.

Utama, S., Din, R., & Mahmuddin, M. (2017). The Performance Evaluation of Feature-Based Technique in Text Steganography. *Journal of Engineering Science and Technology*, *12*, 169–180.

Valandar, M. Y., Ayubi, P., & Barani, M. J. (2017). A new transform domain steganography based on modified logistic chaotic map for color images. *Journal of Information Security and Applications*, *34*, 142–151. https://doi.org/10.1016/j.jisa.2017.04.004

Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H., & Sun, J. (2022). A comprehensive survey on robust image watermarking. *Neurocomputing*, *488*, 226–247. https://doi.org/10.1016/j.neucom.2022.02.083

Wang, J., Zhu, Y., Ni, J., Wang, H., & Yao, Y. (2023). Text Coverless Information Hiding Based on the Combination of Chinese Character Components. *Journal of Circuits, Systems and Computers*, *32*(3), 2023. https://doi.org/10.1142/S021812662350055X

Wu, H. T., Cheung, Y. ming, Yang, Z., & Tang, S. (2019). A high-capacity reversible data hiding method for homomorphic encrypted images. *Journal of Visual Communication and Image Representation*, *62*, 87–96. https://doi.org/10.1016/j.jvcir.2019.04.015

Wu, N., Shang, P., Fan, J., Yang, Z., Ma, W., & Liu, Z. (2019a). Coverless Text Steganography Based on Maximum Variable Bit Embedding Rules. *Journal of Physics: Conference Series*, *1237*, 022078. https://doi.org/10.1088/1742-6596/1237/2/022078

Wu, N., Shang, P., Fan, J., Yang, Z., Ma, W., & Liu, Z. (2019b). Research on

Universiti Utara Malaysia

Coverless Text Steganography Based on Single Bit Rules. *Journal of Physics: Conference Series*, *1237*, 022077. https://doi.org/10.1088/1742-6596/1237/2/022077

Wu, N., Yang, Y., Li, L., Yang, Z., Shang, P., Ma, W., & Liu, Z. (2020). Coverless text hiding method based on improved evaluation index and one-bit embedding. *CMES - Computer Modeling in Engineering and Sciences*, *124*(3), 1035–1048. https://doi.org/10.32604/cmes.2020.010450

Wu, N., Yang, Z., Yang, Y., Li, L., Shang, P., Ma, W., & Liu, Z. (2020). STBS-Stega: Coverless text steganography based on state transition-binary sequence. *International Journal of Distributed Sensor Networks*, *16*(3). https://doi.org/10.1177/1550147720914257

Yang, Z., He, J., Zhang, S., Yang, J., & Huang, Y. (2021). *TStego-THU: Large-Scale Text Steganalysis Dataset BT - Advances in Artificial Intelligence and Security* (X. Sun, X. Zhang, Z. Xia, & E. Bertino (eds.); pp. 335–344). Springer International Publishing.

Yang, Z., Huang, Y., & Zhang, Y.-J. (2019). A Fast and Efficient Text Steganalysis Method. *IEEE Signal Processing Letters*, *26*(4), 627–631. https://doi.org/10.1109/LSP.2019.2902095

Yang, Z. L., Guo, X. Q., Chen, Z. M., Huang, Y. F., & Zhang, Y. J. (2019). RNN-Stega: Linguistic Steganography Based on Recurrent Neural Networks. *IEEE Transactions on Information Forensics and Security*, *14*(5), 1280–1295. https://doi.org/10.1109/TIFS.2018.2871746

Yu, L., Lu, Y., Yan, X., & Wang, X. (2022). Generative Text Steganography via Multiple Social Network Channels Based on Transformers. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13551 LNAI*, 606–617. https://doi.org/10.1007/978-3-031-17120-8_47

Yu, L., Lu, Y., Yan, X., & Yu, Y. (2022). MTS-Stega: Linguistic Steganography Based on Multi-Time-Step. *Entropy*, *24*(5), 1–16. https://doi.org/10.3390/e24050585

Zhang, C., Wang, X., & Sun, W. (2021). Coverless Steganography Method based on

the Source XML File Organization of OOXML Documents. *Proceedings - 2021 2nd International Conference on Electronics, Communications and Information Technology, CECIT 2021*, 413–420. https://doi.org/10.1109/CECIT53797.2021.00080

Zhang, Y., Luo, X., Wang, J., Lu, W., Yang, C., & Liu, F. (2022). Research progress on digital image robust steganography | 数字图像鲁棒隐写综述. *Journal of Image and Graphics*, *27*(1), 3–26. https://doi.org/10.11834/jig.210449

Zhu, J., Zhang, Y., Liu, Z., & Zhang, X. (2022). A Steganographic System based on "Martian" Generation for Avoidance of Text Information Interception. *Journal of Cyber Security*, *7*(5), 1–18. https://doi.org/10.19363/J.cnki.cn10-1380/tn.2022.09.01

Universiti Utara Malaysia