VISUAL CRYPTOGRAPHY FOR E-VOTING BY USING FINGERPRINT TECHNIQUE

HADI RATHAM GHAYAB

UNIVERSITI UTARA MALAYSIA
September 2010

VISUAL CRYPTOGRAPHY FOR E-VOTING

BY USING FINGERPRINT TECHNIQUE

A project submitted to Dean of Postgraduate Studies and Research
In partial fulfillment of the requirements for the degree
Master of Sciences of (Information Technology)
University Utara Malaysia

By

HADI RATHAM GHAYAB

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certifies that)

HADI RATHAM GHAYAB
(802823)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project of the following title)

VISUAL CRYPTOGRAPHY FOR E-VOTING
BY USING FINGERPRINT TECHNIQUE

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that this project is in acceptable form and content, and that a satisfactory knowledge of the field is covered by the project).

Nama Penyelia
(Name of Supervisor) : **ASSOC. PROF. HATIM MOHAMAD TAHIR**

Tandatangan
(Signature) : _____ Tarikh (Date) : 14/10/2010

Nama Penilai
(Name of Evaluator) : **MR. ALI YUSNY DAUD**

Tandatangan
(Signature) : _____ Tarikh (Date) : 14/10/2010

PERMISSION TO USE

In presenting this project in partial fulfillment of the requirements for a postgraduate degree from the University Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor, in his absence, by the dean of the Faculty of Information Technology. It is understood that any copying or publication or use of this project or parts thereof for financial gain should not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my project.

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

Dean of Research & Postgraduate Studies

College of Arts & Sciences

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman

Malaysia

ABSTRACT

Democracy and elections have more than 2,500 years of tradition. Technology has always influenced the form of elections and the complexity of ways. Performing a good security analysis in the design of the system is a necessary step in order to ensure a reasonable level of protection. In this paper, we decided to use the fingerprint on the electronic voting system to increase the speed and accuracy in the proceedings of the electoral process, with the construction of a high-protection system based on fingerprint voters to give most reliable results, and tries to automation of the electoral system in Iraq, and gains the advantage of an e-voting system.

ACKNOWLEDGMENT

بسم الله الرحمن الرحيم

I humbly thank Allah Almighty, the Merciful and Beneficent, who gave me health, thoughts and co-operative people to me achieve this goal.

I wish to dedicate this work to Holy Prophet Muhammad (peace be upon him) and his companions who laid foundation of modern cultural and physical revolution.

Also I wish to dedicate this work to my father, my Mother my Brothers, and my sisters for their never ending moral support and prayers which always acted as a catalyst in my academic life.

I am heartily thankful to my supervisor, ASSOC. PROF. HATIM MOHAMAD TAHIR for his assistance, guidance and support during the project. Furthermore, my sincere thanks to Mr. ALI YUSNY for giving me idea and comments in making this project right on track.

To my Mother, for her presence, graciousness, and love which motivated me to finish my project, she has always followed me very closely, even though when she was thousands of miles away.

Finally, I offer my regards and blessings to all of those who supported me in any respect during the completion of the research they are (Hayder Khodair, Gza, Moayad Hamed, Aymen Shawkat, Khaled Hussain, Ahmad R., Nassir J., Aqeel S., Anwar A. and Hayder H.) And those who could not mentioned thanks for their support to me and to all my friends in Iraq and my friends in Malaysia.

HADI RATHAM GHAYAB AL-MARSHAD

TABLE OF CONTENTS

CHAPTER THREE

METHODOLOGY

CHAPTER FOUR

DATA ANALYSIS AND DESIGN

LIST OF FIGURE

LIST OF TABLE

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

E-voting (electronic voting) is a relatively new concept, based on your application, which aims to reduce errors and increase the comfort and integrity of the electoral process. The use of electronic voting systems led to a split, as some countries use these systems, and others do not (Abu, Knight, & Refai (2010)).

E-voting is an election method in which the votes are cast or collected by electronic means. The computer system in which the main component is a software component that displays the electronic voting procedure, called the electronic voting system. Direct recording electronic machine is a special case of this system, because it implements all phases of the voting process, from registration and ballot counting (Ondrisek 2009).

E-voting also increasingly gains interest in e-democracy and e-government movements. Not only the security and availability of electronic voting systems are of paramount importance, and scalability is of great interest. Especially the fact that in political elections the system has to scale nation-wide, thus having several millions of users (Rossler, Leitold, & Posch 2005).

The contents of the thesis is for internal user only

REFERENCES

Abu-Shanab E., Knight M. & Refai H. (2010). E-Voting Systems: A Tool For E-Democracy. *Management Research and Practice, 2* (3).

Adnan, W., Siang, L., & Hitam, S (2004). Fingerprint recognition in wavelet domain. *Jurnal Teknologi, 41,* 25-42.

Barry, B. (2000). *Spiral model.* Retrieved June 20, 2010 from, http://encyclopedia.thefreedictionary.com/Spiral%20model

Boehm, B., & Abts, C. (1999). COTS integration: Plug and Pray?. *Computer, 32*(1), 135-138.

Bryans, J. W., Littlewood, B., Ryan, P. Y. A., & Strigini, L. (2006). *E-voting: dependability requirements and design for dependability.* Paper presented at the The First International Conference on Availability, Reliability and Security, on ARES 08 May 2006, Newcastle upon Tyne Univ., UK..

Buldas, A., & Mägi, T. (2007). *Practical security analysis of e-voting systems.* Paper presented at the Proceedings of the Security 2nd international conference on Advances in information and computer security 2007, Tallinn, Estonia.

Carrillo, M. (2003). Continuous biometric authentication for authorized aircraft personnel: A proposed design. Unpublished master thesis USA: New Mexico State University, Monterey, California.

Cha, B., & Kim, C. (2008). *Password Generation of OTP System using Fingerprint Features.* Paper presented at the International Conference on Information Security and Assurance 07 May 2008, Busan.

Esposito, D. (2002). *Building web solutions with ASP .NET and ADO .NET.* WA, USA: Microsoft Press Redmond.

Gallegos-Garcia, G., Gomez-Cardenas, R., & Duchen-Sanchez, G. (2010). *Electronic Voting Using Identity Based Cryptography.* Paper presented at the Fourth International Conference on Digital Society 18 March 2010, St. Maarten.

Gibson, J., Lallet, E., & Raffy, J. (2008). *Analysis of a distributed e-voting system architecture against quality of service requirements.* Paper presented at the The Third International Conference on Software Engineering Advances, 2008. ICSEA'08, Sliema.

Hamilton, M. (1999). Software development: building reliable systems. *Prentice Hall Enterprise Computing Series*, 357.

Hidano, S., Ohki, T., Komatsu, N., & Kasahara, M. (2008*). On biometric encryption using fingerprint and it's security evaluation.* Paper presented at the 10th International Conference on Control, Automation, Robotics and Vision, 27 Feb 2009. ICARCV 2009, Hanoi.

Hu, C., & Tzeng, W. (2007). Cheating prevention in visual cryptography. *IEEE Transactions on Image Processing, 16*(1), 36-45.

Hubbers, E., Jacobs, B., & Pieters, W. (2005*).* RIES-internet voting in action. *Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05), IEEE CS Press, 1,* 417-424.

Hudgins, K., & Hudgins, M. (2002). *Experiential treatment for PTSD: The therapeutic spiral model.* New York: Springer Publishing Company.

Kalvet, T. (2009). Management of Technology: *The Case of e-Voting in Estonia.* Paper presented at the International Conference on Computer Technology and Development 28 Dec 2009, Kota Kinabalu.

Katzman, K. (2010). *Iraq: Politics, Elections, and Benchmarks.* New York: Congressional Research Service.

Khasawneh, M., Malkawi, M., Al-Jarrah, O., Barakat, L., Hayajneh, T., & Ebaid, M. (2008). *A biometric-secure e-voting system for election processes.* Paper presented at the 5th International Symposium on Mechatronics and Its Applications, 14 Oct 2008. ISMA 2008, Amman.

Kohno, T., Stubblefield, A., Rubin, A., & Wallach, D. (2004*). Analysis of an electronic voting system.* Paper presented at Proceedings of Symposium on Security and Privacy, 01 Jun 2004 IEEE, California Univ., San Diego, CA, USA.

Lamon, P., Nourbakhsh, I., Jensen, B., & Siegwart, R. (2001). Deriving and matching image fingerprint sequences for mobile robot localization. *IEEE International Conference on Robotics and Automation, 2,* 1609-1614

Lee, S., Choi, H., Choi, K., & Kim, J. (2008). Fingerprint-quality index using gradient components. *IEEE Transactions on Information Forensics and Security, 3*(4), 792-800.

Leon, D., & Podgurski, A. (2003*). A comparison of coverage-based and distribution-based techniques for filtering and prioritizing test cases.* Paper presented at the 14th International Symposium on Software Reliability Engineering, 08 Dec 2003. ISSRE 2003, Cleveland, OH, USA.

Liu, F., Wu, C., & Lin, X. (2008). Colour visual cryptography schemes. *Information Security, IET, 2*(4), 151-165.

Liu, F., Wu, C., & Lin, X. (2010). Step construction of visual cryptography schemes. *IEEE Transactions on Information Forensics and Security, 5*(1), 27-38.

Malkawi, M. (2008). *A Biometric-Secure e-Voting System for Election Processes.* Paper presented at the 5th International Symposium on Mechatronics and Its Applications, 14 Oct 2008. ISMA 2008, Amman.

Mercuri, R. (2001). *Electronic vote tabulation checks and balances.* Dissertations available from ProQuest. Retrieve on 3 July 2001 from, http://repository.upenn.edu/dissertations/AAI3003665

Naor, M., & Shamir, A. (1997). *Visual cryptography II: Improving the contrast via the cover base.* New York: Springer.

Omidi, A., & Azgomi, M. (2009). *An architecture for e-voting systems based on dependable web services.* Paper presented at the Proceedings of the 6th international conference on Innovations in information technology 05 April 2010, Al Ain.

Ondrisek, B (2009*). E-voting system security optimization.* Paper presented at the 42nd Hawaii International Conference on System Sciences, 20 Jan 2009. HICSS '09, Big Island, HI.

Rao, M., Sukonkina, M., Bhagwati, C., & Singh, M. (2008). *Fingerprint based authentication application using visual cryptography methods.* TENCON 2008 - 2008 IEEE Region 10 Conference, 27 Jan 2009, Hyderabad.

Rossler, T., Leitold, H., & Posch, R. (2005). *E-voting: A scalable approach using XML and hardware security modules.* Paper presented at the Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05) on e-Technology, e-Commerce and e-Service 11 April 2005, Austria.

Rothermel, G., Untch, R., Chu, C., & Harrold, M. (2001). Prioritizing test cases for regression testing. *IEEE Transactions on Software Engineering*, 929-948.

Rubin, A. (2002). Security considerations for remote electronic voting. *Communications of the ACM, 45*(12), 44

Sleit, A., Amman, J., & Abusitta, A (2007). A Visual Cryptography Based Watermark Technology for Individual and Group Images. *Systemics, Cybernetics And Informatics, 5*(4), 24-32

Sugiura, A., & Koseki, Y. (1998). *A user interface using fingerprint recognition: holding commands and data objects on fingers.* Paper presented at the Proceedings of the 11th annual ACM symposium on User interface software and technology 1998, New York, NY, USA.

Weldemariam, K., Mattioli, A., & Villafiorita, A., (2009). *Managing Requirements for e-voting Systems: Issues and Approaches Motivated by a Case Study.* Center for Information Technology, FBK-IRST 2009, Italy.

Wen, C., Guo, T., & Wang, S. (2009). *Fingerprint Feature-Point Matching Based on Motion Coherence.* Paper presented at the Second International Conference on Future Information Technology and Management Engineering 15 Jan 2010, Sanya.

Wu, J., Xie, S., Seo, D., & Lee, W. (2008). *A New Approach for Classification of Fingerprint Image Quality.* Paper presented at the 7th IEEE International Conference on Cognitive Informatics, 2008. ICCI 07 Oct 2008, Stanford, CA.

Yong-Sork, H., & Sakurai, K, (2002). The Analysis of Current State and Future on the E-voting System. *Symposium on Cryptography and Information Security, 1*, 537-542

Younhee, G., Dosung, A., Sungbum, P., & Yongwha, C. (2003). *Access control system with high level security using fingerprints.* Paper presented at the 32nd Proceedings Applied Imagery Pattern Recognition Workshop, 13 April 2004, Taejon, South Korea.

Zhou, Z., Arce, G., & Di Crescenzo, G. (2006). Halftone visual cryptography. *IEEE Transactions on Image Processing, 15*(8), 2441-2453