“I declare that I have read this project, in my opinion this project report has satisfied the scope and quality for the award of the degree of Master of Computer Science (Information Security).”

Signature :
Name of Supervisor : DR. MAZDAK ZAMANI
Date : JUNE 2013

AN ENHANCED CHAOTIC ENCRYPTION METHOD FOR FRAGILE WATERMARKING

SIMA BOUJARIAN

A PROJECT SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF
MASTER OF COMPUTER SCIENCE (INFORMATION SECURITY)

ADVANCED INFORMATICS SCHOOL
UNIVERSITI TEKNOLOGI MALAYSIA

JUNE 2013

I declare that this thesis entitled: “AN ENHANCED CHAOTIC ENCRYPTION METHOD FOR FRAGILE WATERMARKING” is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is degree and is not concurrently submitted in candidature of any other degree.

Signature :
Name : SIMA BOUJARIAN
Date : 19th JUNE 2013

Dedicated to

My Beloved Parents and My darling supportive Brothers

ACKNOWLEDGEMENT

IN THE NAME OF GOD, MOST GRACIOUS, MOST COMPASSIONATE

May I express my appreciation to GOD, for giving me the blessing for health, strength and earnestness to accomplish and fulfill this project report.

I am very fortunate to have had Dr. Mazdak Zamani as my supervisor. I am deeply indebted to him whose guidance, inspiration, and suggestions helped me finish this work. I would like to express my deepest appreciation to him. I appreciate Universiti Teknologi Malaysia, and Advanced Software Engineering Faculty of Computer Science and Information System. I am grateful to all my friends who made the times I spent in this university both rewarding and enjoyable.

This appreciation also goes to my beloved mother and brothers, because of their uninterrupted support during my study and my dearest friends Tanya Koohpahey that accompanied me in all times and also my dear friend Abang Abdul Rasyd for translating project abstract to Malay.

ABSTRACT

These days internet is one of the most important part of human life and the most significant issue that is connected to this technology is keeping data secure. Many attackers try to obtain secret information for different reason so sometimes it is necessary to keep existence of data secret. Cryptography and watermarking can combine to each other to create a secure platform for sensitive information. In some model even after combining encryption and watermarking the hidden message can be detectable. In our proposed model two type of encryption methods which are Arnold Cat Map and RSA algorithm are combined with LSB watermarking to make hidden message secure. This method creates confusion and diffusion to keep existence of information secure. Results show that the proposed model increase security of hidden message with lower time of implementation algorithm.

ABSTRAKT

Internet hari ini merupakan antara perkara paling penting dalam kehidupan manusia. Ianya juga merupakan isu paling penting kerana memastikan teknologi memelihara data terpelihara. Banyak penggodam cuba mendapatkan maklumat rahsia dengan alasan tersendiri maka ianya menjadi kewajipan untuk kita mempunyai sebuah platform yang selamat untuk maklumat yang sensitive. Dalam beberapa model sebelumnya, mesej rahsia masih boleh dikesan meskipun selepas menggabungkan kaedah *encryption* dan *watermark*. Dalam model yang dicadangkan, terdapat dua jenis kaedah encryption iaitu Arnold Cat Map dan algoritma RSA yang digabungkan dengan watermarking LSB untuk menjadikan maklumat rahsia. Kaedah ini menimbulkan kekeliruan dan penyebaran untuk meastikan kewujudan maklumat adalah selamat. Hasil kajian menunjukkan bahawa model yang dicadangkan meningkatkan keselamatan mesej rahsia dengan masa yang lebih singkat bagi perlaksanaan algoritma.

CHAPTER 1

INTRODUCTION

1.1 Overview

These days every one can access to huge amount of digital data easily. Rapid growth of internet technologies has changed our world. There are varieties of data that transfer every second in all over the world during this communication these data could be misused in different ways for different goals. In recent year's digital multimedia and influential image processing tools can change digital data and make manipulating and tampering(W. Lin *et al.*, 2011 and Lu and Liao, 2003).

Some on new technologies have been used to prevent illegal activities, such as cryptography, but this problem cannot be solved by this technology alone, because data encryption only provide security during transmission of data and when data is received and decrypted, the product will no longer be secured. This problem is solved by proposing a new effective copyright protection of digital information and a technique for data security maintenance, digital watermark technology(Kumar, Sampath, and Indumathi, 2012).

According to different types of watermark carrier, digital watermark can be divided into: image watermark, video watermark and audio watermark. In the field of data security, watermarks may be used for certification, authentication, and conditional access(Ali and Khamis, 2012).

There are different reasons for manipulating image in different level of security in different areas. Protecting of data is important issue these days because some of secret data could be misused for sabotage or terrorism, or military and political reason that is so important and could effect in all people lives(Ying-Da Lv, Shen, and Chen).

Authenticity of image content and verification of integrity are so important because manipulating images are so easy. Protection of digital image and determine manipulation is very noticeable issue as a large number of digital images are interchanged on the Internet every day. Today many kind of authentication schemes have been proposed for authenticity and verifying integrity(Friedman, 1993 and W. Lin, *et al.,* 2011).

The authentication methods can be categorized into two categories: Digital signature based schemes and Digital watermark based schemes. A digital signature can be also a signed or an encrypted hash value of image contents or image characteristics. The main disadvantage of signature based schemes is that they can only identify if an image has been modified or not, but they cannot find out the position of the regions that have been modified. To solving this problem, watermark based scheme has been proposed for image authentication(Lu and Liao, 2003 and Rey and Dugelay, 2002).

1.1.1 Reason of information secrecy

People can say that secret communication is necessary for terrorists, drug dealers and many other criminals and also for a war. It is really true, but there are many humanitarian reasons for secrecy too. You can explore job possibilities without revealing where you currently work and potentially losing your job. You can protect you personal information from being exploited by terrorists or money launderers. The police can communicate with undercover agents infiltrating the gangs of bad people. So there are many reasons that protect the solid people(Martin, Sapiro, and Seroussi, 2005).

1.1.2 Principle of Watermarking

A watermarking system is typically separated into three different steps, embedding, attack and detection. In embedding, an algorithm embeds the host and data and a watermarked signal is produced by this algorithm. The watermarked signal is broadcasted or stored after that, but usually it is transmitted to another person, if this person makes a change to this watermark signal this is called an attack. An algorithm that embedding attacked signal for extracting the watermark from it is called detection algorithm. Two things would be happen; if the watermark is still there and could be extracted it means that the signal was not modified but if the signal is copied the information is also transmitted to the copy and the content is manipulated. Figure 1.1 shows the basic block map of watermarking process(Potdar, Han, and Chang, 2005).

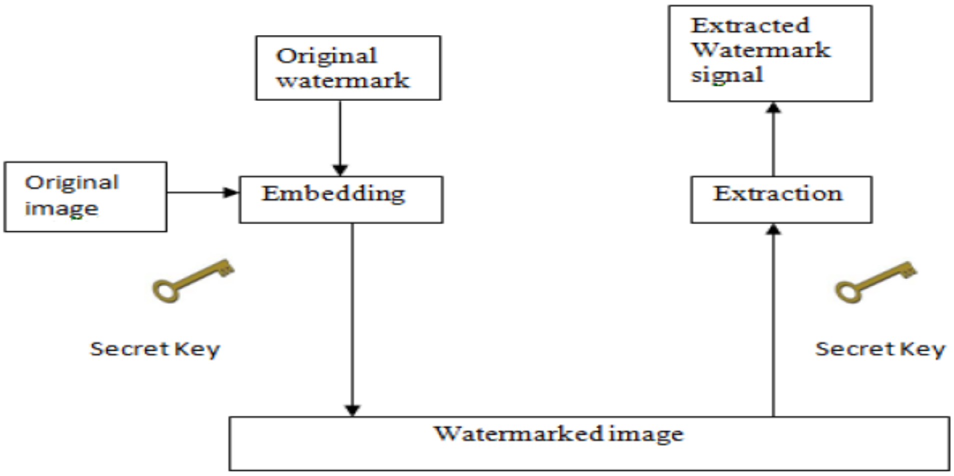

Figure 1.1: Watermarking block map(Potdar, *et al.*, 2005)

Various schemes are accessible to embed the original image and desired watermark. One secret key is used during embedding and extraction process for preventing illegitimate access to the watermark(Potdar, *et al.*, 2005).

1.2 Background of problem

There are many easy ways that help to attackers that can extract hidden message easily by trying extraction algorithm or find out the method approximately by knowing some features of watermarked image like PSNR that is related to quality of image. So it is an important issue to making message as secure as possible to prevent leaking sensitive information(Cheddad, Condell, Curran, and Mc Kevitt, 2010).

One of the chaotic method encryption that had been used in image watermark security is Arnold Cat Map encryption method that scrambles image pixels position and after applying Arnold Cat Map for T times pixels of image will return back to the original place. This T is related to the size of image and is different for different sizes but it is not very large number. Arnold Cat Map had been used for scrambling image K times which K is defined as encryption key and the message will be embed in image that had been scrambled K times and after embedding, carrier will be scrambled (T-K)times because the image pixel come back to the original place. This method helps to increase security of message because even if attacker can be able to extract message the pixels of it is not in right place, but since amount of T is not huge and can be detectable by image size(Rawat and Raman, 2011 and Struss, 2009).

1.3 Problem statement

As it was mentioned in background of problem by fining period duration for Arnold cat Map is not a big number and amount of K that s the encryption key can be easily find by try and failure. When attacker succeed to find K it would be very easy for her/him to extract the message from carrier and the secret message would be recognizable for attackers so Arnold Cat Map is not efficient for guarantee security of hidden message.

1.4 Project objectives

The project objectives of this project are as bellow:

1. To investigate existing method based on fragile watermarking for secure hidden message.
2. To proposed and enhance fragile watermarking model to secure hidden watermark
3. To test and evaluate existing models with proposed model.

1.5 Project aim

The aim of this project is to provide secure model for image watermarking.

1.6 Project scope

The scope of this research is based on ivisible fragile watermarking that focuses on increasing security by using encryption and watermark based on spatial domain watermark. There are different methods in spatial domain that in this project the method that is proposed is focused on LSB method that used least significant bits for embedding the watermark. Another method that would be used for creating watermark is using chaotic encryption that makes confusion and diffusion for making hidden message more secure. The image that would be embedding in carrier is bmp gray scale image in size of 256×256 pixel that will be hidden behind image with size of 512*512. For implementation of this project MATLAB software would be used and version that is used in this project is R2011b version 7.13.5604.

1.7 Summary

Watermarking is very important part of hiding area and there are many research subjects Digital watermarking can be used for various areas like provide security to information that are transferring on network these days. For more effectiveness of watermarking it is better that watermarking will be combined by cryptography method.

REFERENCES

Al-Najjar, H. M. Digital Image Encryption Algorithm Based on a Linear Independence Scheme and the Logistic Map.

Al-Otum, H. A., and Al-Taba'a, A. O. (2009). Adaptive color image watermarking based on a modified improved pixel-wise masking technique. *Computers & Electrical Engineering, 35*(5), 673-695.

Ali, H. A., and Khamis, S. A. K. (2012). *Robust Digital Image Watermarking Technique Based on Histogram Analysis.* Paper presented at the First National Scientific Conference for Computer Science and Technology, Basrah University.

Anane, N., Anane, M., Bessalah, H., Issad, M., and Messaoudi, K. (2010). *RSA based encryption decryption of medical images.* Paper presented at the Systems Signals and Devices (SSD), 2010 7th International Multi-Conference on.

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

Chen, B., and Shen, H. (2009). *A new robust-fragile double image watermarking algorithm.* Paper presented at the Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on.

Cummins, J., Diskin, P., Lau, S., and Parlett, R. (2004). Steganography and digital watermarking. *School of Computer Science, The University of Birmingham*.

Cummins, J., Diskin, P., Lau, S., and Parlett, R. (2004). Steganography and digital watermarking. *School of Computer Science, The University of Birmingham, 14*, 60.

De Strycker, L., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M.*, et al.* (2000). *Implementation of a real-time digital watermarking process for broadcast monitoring on a TriMedia VLIW processor.* Paper presented at the Vision, Image and Signal Processing, IEE Proceedings-.

Di Martino, F., and Sessa, S. (2012). Fragile watermarking tamper detection with images compressed by fuzzy transform. *Information Sciences*.

Friedman, G. L. (1993). The trustworthy digital camera: Restoring credibility to the photographic image. *Consumer Electronics, IEEE Transactions on, 39*(4), 905-910.

Gao, H., Zhang, Y., Liang, S., and Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons & Fractals, 29*(2), 393-399.

Gong-bin, Q., Qing-feng, J., and Shui-sheng, Q. (2009). *A new image encryption scheme based on DES algorithm and Chua's circuit.* Paper presented at the Imaging Systems and Techniques, 2009. IST'09. IEEE International Workshop on.

Jain, P., and Rajawat, A. S. Fragile Watermarking for Image Authentication: Survey.

Johnson, W. N. H., Blackledge, J. M., and Murray, B. L. J. (2003). Applications of fractal and/or chaotic techniques: Google Patents.

Keyvanpour, M., and Farnoosh, M. (2010). *A new encryption method for secure embedding in image watermarking.* Paper presented at the Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on.

Khammar, M. R., Saied, Y. A., and Marhaban, M. (2011). A Digital Image Watermarking Method in the Discrete Cosine Transformation Domain. *International Journal on Advanced Science, Engineering and Information Technology, 2*(1), 96-100.

Khan, A., and Mirza, A. M. (2007). Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. *Information Fusion, 8*(4), 354-365.

Kumar, R. R., Sampath, A., and Indumathi, P. (2012). Image Encryption using Watermarking and Chaotic Maps. *European Journal of Scientific Research, 84*(1), 130-138.

Lee, S. J., and Jung, S. H. (2001). *A survey of watermarking techniques applied to multimedia*.

Lin, T. C., and Lin, C. M. (2009). Wavelet-based copyright-protection scheme for digital images based on local features. *Information Sciences, 179*(19), 3349-3358.

Lin, W., Tao, D., Kacprzyk, J., Li, Z., Izquierdo, E., and Wang, H. (2011). *Multimedia Analysis, Processing and Communications* (Vol. 346): Springer.

Lu, C. S., and Liao, H. Y. M. (2003). Structural digital signature for image authentication: an incidental distortion resistant scheme. *Multimedia, IEEE Transactions on, 5*(2), 161-173.

Malshe, S., Gupta, H., and Mandloi, S. (2012). Survey of Digital Image Watermarking Techniques to achieve Robustness. *International Journal of Computer Applications, 45*(13), 1-8.

Martin, A., Sapiro, G., and Seroussi, G. (2005). Is image steganography natural? *Image Processing, IEEE Transactions on, 14*(12), 2040-2050.

Miller, M. L., Cox, I. J., Linnartz, J. P. M. G., and Kalker, T. (1999). A review of watermarking principles and practices. *Digital Signal Processing for Multimedia Systems*, 461-485.

Mishra, M., Routray, A. R., and Kumar, S. (2012). High Security Image Steganography with Modified Arnold's Cat Map. *International Journal of Computer Applications, 37*(9).

Mohanty, S. P., Ramakrishnan, K., and Kankanhalli, M. (1999). *A dual watermarking technique for images*.

Neeta, D., Snehal, K., and Jacobs, D. (2006). *Implementation of LSB steganography and its evaluation for various bits*.

Popa, R. (1998). An analysis of steganographic techniques. *The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering*.

Potdar, V. M., Han, S., and Chang, E. (2005). *A survey of digital image watermarking techniques*.

Ptitsyn, N. V., Blackledge, J. M., and Chernenkiyt, V. M. (2002). *Deterministic chaos in digital cryptography*. Paper presented at the Proceedings of the First IMA Conference on Fractal Geometry: Mathematical Methods, Algorithms and Applications (Eds. JM Blackledge, AK Evans and M Turner), Horwood Publishing Series in Mathematics and Applications.

Qiang, S., and Hongbin, Z. (2010). *Image Tamper Detection and Recovery Using Dual Watermark.* Paper presented at the Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on.

Radharani, S., and Valarmathi, M. (2010). A Study on Watermarking Schemes for Image Authentication. *International Journal of Computer Applications IJCA, 2*(4), 24-32.

Rawat, S., and Raman, B. (2011). A chaotic system based fragile watermarking scheme for image tamper detection. *AEU - International Journal of Electronics and Communications, 65*(10), 840-847.

Rey, C., and Dugelay, J. L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing, 2002*(1), 613-621.

Struss, K. (2009). *A Chaotic Image Encryption.* Paper presented at the Spring, Mathematics Senior Seminar.

Syed, A. A. (2011). Digital Watermarking. *The University of Texas at Arlington*.

Wu, X., and Guan, Z.-H. (2007). A novel digital watermark algorithm based on chaotic maps. *Physics Letters A, 365*(5), 403-406.

Yang, C. N., and Lu, Z. M. (2011). A Blind Image Watermarking Scheme Utilizing BTC Bitplanes. *International Journal of Digital Crime and Forensics (IJDCF), 3*(4), 42-53.

Yeung, M. M., and Mintzer, F. (1997). *An invisible watermarking technique for image verification*.

Ying-Da Lv, A., Shen, B. X. J., and Chen, C. H. P. Blind Identification of Image Copy-paste Tampering Based on Logarithm Polar Coordinate Transformation.

Yun-peng, Z., Wei, L., Shui-ping, C., Zheng-jun, Z., Xuan, N., and Wei-di, D. (2009). *Digital image encryption algorithm based on chaos and improved DES.* Paper presented at the Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on.

Zhang, D., Pan, Z., and Li, H. (2010). *A Contour-Based Semi-fragile Image Watermarking Algorithm in DWT Domain.* Paper presented at the Education Technology and Computer Science (ETCS), 2010 Second International Workshop on.

Zhao, G., Yang, X., Zhou, B., and Wei, W. (2010). *RSA-based digital image encryption algorithm in wireless sensor networks.* Paper presented at the Signal Processing Systems (ICSPS), 2010 2nd International Conference on.