A GRAY-SCALE IMAGE STEGANOGRAPHY TECHNIQUE USING FIBONACCI 12-BITPLANE DECOMPOSITION AND LSB APPROACH

SABAH FADHEL HAMOOD

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

FEBRUARY 2013

This dissertation is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor **Prof. Dr. Ghazali Bin Sulong** for his constant support during my study at UTM. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

After the great expansion of internet, communications tends to be lifeblood, at the same time data protection became more critical issue, so the need to secure transfer channel is being more urgent, this goal achieved by applying one or more of data protection techniques. Steganography one of the most suitable solution for this problem, due to the good specification of concealing secret file inside cover image, in such way there is nobody even suspects the existence of transferred file. The main challenge in steganography methods is how to make balance between the quality of file that will be used to conceal the secret and the size of the secret file. Also there are another factors should be considered, which are, robustness and security against attacks. In this study Fibonacci numbers have been exploited to achieve these goals. Fibonacci numbers used to decompose the cover file into 12-bitplanes instead of 8-bitplanes produced by binary decomposition, the four extra layers will increase the capacity of cover image. The resulted 12-bitplanes, has special statistical nature in terms of distribution of black regions (zero values) and white regions (one values). This statistical nature has been exploited by modifying the binary representation of secret message to make matching between the representation of secret message and cover image to reduce the impact of embedding process on the resulted file (stego-image). By applying Fibonacci decomposition to the cover image, better results have been achieved in terms of Peak Signal to Noise Ratio(PSNR) which indicates the ability of embed more secret size with maintaining the quality of stego-image, also the security and robustness has been evaluated by applying chi-square attack, the result for this attacks show that Fibonacci LSB method is withstanding for such attack.

ABSTRAK

Selepas internet berkembang dengan pesatnya, komunikasi telah menjadi nadi, dalam masa yang sama perlindungan data menjadi isu yang lebih kritikal, jadi keperluan untuk mendapatkan saluran pemindahan menjadi lebih penting, matlamat ini dicapai dengan menggunakan satu atau lebih teknik perlindungan data. Steganografi adalah salah satu penyelesaian yang paling sesuai untuk masalah ini, disebabkan oleh penyembunyian fail rahsia yang baik di dalam fail biasa (fail pelindung), dengan cara itu tiada siapa yang akan mengesyaki walaupun fail dipindahkan. Cabaran utama dalam kaedah steganografi adalah bagaimana untuk membuat keseimbangan antara kualiti fail yang akan digunakan untuk menyembunyikan rahsia dan saiz fail rahsia tersebut. Juga terdapat faktor-faktor lain yang perlu dipertimbangkan apabila teknik steganografi digunakan, faktor ini adalah kekukuhan rahsia tersembunyi dan keselamatan penerapan teknik serangan yang dijangka terhadap musuh. Untuk mencapai matlamat ini, nombor Fibonacci telah dikaji. Nombor Fibonacci digunakan untuk menguraikan fail perlindungan ke 12-bitplanes bukannya 8-bitplanes yang dihasilkan oleh penguraian binari, empat lapisan tambahan akan membawa kepada peningkatan kapasiti fail perlindungan. Kesimpulan untuk 12-bitplanes, mempunyai sifat statistik khas dari segi bentuk kawasan hitam (nilai sifar) dan kawasan-kawasan putih (satu nilai). Sifat khas ini telah disalah guna dengan mengubah sifat fail rahsia khas tersebut untuk membuat padanan antara sifat khusus fail rahsia dan fail perlindungan dan untuk mengurangkan kesan proses penerapan pada fail akhir (stego fail). Dengan menggunakan penguraian Fibonacci kepada imej penutup, keputusan yang lebih baik telah dicapai dari segi Isyarat Puncak kepada Nisbah Bunyi (PSNR).

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

LSB	Least significant Bit
HVS	Human Visual System
PVD	Pixel Value Differencing method
MBNS	Multiple-Base Notational System
DCT	Discrete Cosine Transform
XML	Extensible Markup Language
JPEG	Joint Photographic Expert Group
GIF	Graphic Interchange Format
Bmp	Bitmap image format
OSI	Open Systems Interconnection
TCP/IP	Internet protocol suite TCP/IP
HAD	Human Audio System
PSNR	peak signal to noise ratio
MSE	Mean Square Error
SLSB	Selected Least Significant Bit
PVD	Pixel-Value Differencing
PRNG	Pseudo-Random Number Generator
RGB	Red Green Blue

CHAPTER 1

INTRODUCTION

1.1 Introduction

Several years ago, an issue which has preoccupied the attention and thinking of a lot people especially, in the military and political fields, is the data hiding technique for the confidentiality of their information. This is more crucial for the Middle East region, because of unstable political situations. The Middle East, being the center of the Islamic world plus possessing more than 60% of the world's oil therefore, the concern to find secure ways to send information is very important. Thus, there were always methods and secret means that were followed to sending these secret data. After the expansion of internet applications, information sending has become quick and easy. Parallel to that, hackers were easily uncovered and intercepted the sent data (Khalaf and Sulaiman, 2011).

One method of providing more security to data is information hiding, which is the field of securing communication using cryptography, the cryptography approach deals with the encryption of data at the sender’s side and the decryption of data at the receiver’s side. Steganography is also used for secret data transmission; the main difference between steganography and cryptography is the suspicion factor. When steganography and cryptography are implemented together, the level of security will increase. Steganography makes the presence of the secret data appear invisible to eavesdroppers such as, key loggers or harmful tracking cookies where the users’ keystrokes are monitored while entering password and personal information. So, “Steganography, is the art and science of hiding information, in such a way that, its presence cannot be detected” (Ramkumar and Akansu, 1999). Steganography used for hiding and sending data apparently using innocuous carriers to conceal even the existence of the secret message (Petitcolas et al., 1999). The goal of applying steganography is to make message communications in such secure and completely undetectable way (Provos and Honeyman, 2003),(Amin et al., 2003).

The techniques of data hiding embed the confidential data into a multimedia file such as video, images or sounds. The suitable cover signal is the digital image, due to their insensitivity to human visual system HVS(Mohamed et al., 2011). The word steganography “comes from Greek; stegano, which means covered or secret and –graphy means writing or drawing. Therefore, steganography literally means “covered writing”(Ramkumar and Akansu, 1999).

Steganography was developed centuries ago, but in recent decades has been studied on the consideration of it being one of the areas of science. Nowadays, most information is electronically kept and at the same time, the information security has become an essential issue. Steganography, beside cryptography can be applied to increase information security. Steganography is a method of hiding a secret message in a digital signal. In comparison to cryptography, the secret message or encrypted secret message is embedded into a digital carrier signal before sending it through the network, thus the existence of the secret message is unknown(Ramkumar and Akansu, 1999).

The Steganography goal is to hide secret messages inside another harmless message in a way to not allow hackers to even know that there is a secret message present(Kekre et al., 2008). The LSB replacement/ LSB matching terminology has been discussed by(Sharp, 2001). The algorithm of LSB substitution is the simplest technique for secret message hiding in a carrier signal. The replacement of the least significant bit (LSB) of each pixel by the bit stream of the encrypted message, is applied according to this technique. The authorized recipient can decipher the least significant bit (LSB) of all pixel of the carrier signal using a pre-shared key to extract the secret message. This method of embedding is imperceptible by the human visual system (HVS), because only the least significant bit of pixels is replaced by the secret bit. Therefore, the maximum capacity for this algorithm is only 1 bit for each pixel(Kekre, et al., 2008).

1.2 Background of the Problem

Steganography is a branch of data hiding techniques, it is also considered as the art of secret hiding inside a cover of a carrier signal(Petitcolas, et al., 1999) ,(Wang and Wang, 2004). There are two valuable factors in Steganography which should be applied at all times, first one is the perceptibility impact of the secret embedding process with regards to the imperceptibility of visual/statistical image properties, while the other factor is the amount of embedded information that can be embedded into the cover signal(Zhang and Wang, 2005). When the size of the secret file is larger than usual, it should be divided into a sequence of segments after that, these segments will be embedded into multiple cover images before sending but, multiple images sending to the same destination will increase the suspicion factor, so to solve this problem the capacity of the stego-image needs to be increased.

1.2.1 Low Payload Capacity

The two most famous algorithms in which the stego-image is highly imperceptible and the capacity of embedding process is low, which are Pixel-Value Differencing (PVD) (Wu et al., 2005) and Multiple-Base Notational System (MBNS) (Zhang and Wang, 2005). The maximum of embedding capacity of these two algorithms depend on the cover signal characteristics and it can be different for different cover signals. These two algorithms are based according to HVS. The total numbers of bits that are embedded in each pixel depend on the pixel, if it is in smooth or in edge area. The maximum embedding capacity is equal to 782,320 bits using PVD algorithm when the cover signal (image) is (airplane), while, when the MBNS algorithm is applied using (Man) as the cover image, the maximum embedding capacity is equal to 740,000 bits. There is a fact in steganography technique which is, there will be a trade-off between imperceptibility and payload capacity in the stego-image, the ideal algorithm of Steganography is that, the algorithm that gives imperceptibility with an acceptable level, without losing any of the payload capacity.

1.2.2 Imperceptibility problems

Among the steganographic insertion techniques, there's an important issue, which is the way of embedding a secret message into an 8-bit grayscale image, (which will be considered as a cover signal) in such a technique that cannot be detected by the human visual system (HVS) for the existence of this secret message, without attention to the expected attack like, Chi-square Attack. Most important is the way of getting acceptable imperceptibility and achieving bigger imperceptibility is very important, even if more pixels are used for estimating the capacity for each target pixel.

1.2.3 Robustness Problem

There is another steganographic property that should be considered when steganographic techniques are applied, especially when the least significant bit (LSB) technique is used, this property is known as robustness. The embedding algorithm can be said to be robust if the embedding secret cannot be removed after applying a reliable detection by a targeted attack; when there's full knowledge about the detector, the embedding algorithm (except knowing the secret key), also the knowledge of at least one carrier with the hidden secret(Michaud, 2003).

1.3 Statement of the Problem

The most famous steganography techniques are DCT and LSB. In first one, the coefficient values of DCT of some image squares are changed for the process of embedding the secret message(Johnson et al., 2001). Whereas, in the LSB technique areas inside the cover image are selected by using different techniques, and then the least significant bit is replaced with the data that needs to be embedded.

Using LSB technique with which this approach would be concerned, an image is used to embed the secret data inside it, and then take the values of its gray-scale. An alternation operation of the least significant bit of gray-scale can be easily made and it is undetectable by the human visual system, HVS. So, a stego-image with high imperceptibility will be achieved. Also, as mentioned in(Wang and Wang, 2004), there are some issues in steganography, the main effort for this study is to increase the payload capacity by using Fibonacci sequences and also by using this technique to get a high robustness stego-image. So the decreasing of image distortion and imperceptibility will be considered.

Fibonacci sequences are related to Leonardo Pisano Fibonacci, who was born around 1170 and died around 1250, in Pisa, what is now Italy. He was always travelling in Northern Africa and Europe. Several mathematical notations were written by him; also, he introduced Europe to the numbers of Hindu-Arabic notations. Although his books were transcribed by the hand, they were circulated widely. In one of most famous of his books, Liber Abaci, which was published in 1202, he proposed the following problem: A man puts a pair of rabbits in a place surrounded on all sides by a wall. How many pairs of rabbits can be produced from that pair in a year if it is supposed that every month each pair begets a new pair which from the second month on becomes productive?. Presently, the solution for such problem is known as Fibonacci numbers, or Fibonacci sequence, also there is a mathematical industry that is based on Fibonacci sequence. The internet search for these sequences will match dozens of web sites, and hundreds of material pages today for the solution to this problem. There is even a Fibonacci Association that publishes a scholarly journal, which is Fibonacci Quarterly.

1.4 Research Aim

The main aim of this study is to improve a steganographic method which can embed secret information into a cover image, with high payload capacity using Fibonacci sequences to hide the data within the framework of adopting the classical LSB scheme.

1.5 Objectives of Research

In order to achieve the aim of the study, there are some identified objectives, such as follows:

- To propose improved steganography algorithm based on Fibonacci LSB technique to provide a high embedding capacity.
- To make comparisons between classical LSB technique and Fibonacci-based LSB technique and the proposed technique according to the payload capacity and imperceptibility.
- To evaluate the robustness of the proposed method against Chi-square attack.

1.6 Research Scope

The proposed approach scope is based on the following points:

- The secret message, which is embedded into the cover media will be an arbitrary generated text with lower case letters (a to z) and space (whitespace).
- The cover media that is used for hiding the desired secret data is a standard dataset of (512 x 512) pixels, and 8-bits gray-scale image taken from the data base of USC-SIPI.
- PSNR formula will be used to evaluate the imperceptibility of stego-image in order to compare with previous works.
- Chi-sqaure will be used to evaluate the robustness of the proposed technique.

1.7 Significance of the Research

Due to the expansion in the field of Internet and wide dependence on the internet resources, the World Wide Web has today become non secure in the transfer of data, so the need to make this environment safer has become more urgent and to achieve a secure environment, the implementation of some security technologies has become valuable.

Steganography, being a more secure technology, has been applied to get a secure communication channel between the sender and the receiver using internet as a communication media. Since Steganography is under some vulnerability such as, payload capacity is one of the most important factor in addition to the imperceptibility of the stego-image.

The proposed technique in this study tries to increase the payload capacity in keeping with the imperceptibility at an acceptable level. This result can be achieved by using least significant bit (LSB) insertion based on Fibonacci decomposition, the insertion of secret bits into the (LSB) of Fibonacci representation is accomplished after making a preprocessing for the secret bits to be adaptive for embedding into the cover image with a minimum image distortion, to get a stego-image with high capacity, without losing the imperceptibility.

REFERENCES

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

Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R. and Shamsuddin, M. (2003). Information hiding using steganography. Proceedings of the 2003 *Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on*, 21-25.

Anand, J. V. and Dharaneetharan, G. (2011). New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security. Proceedings of the 2011 *Proceedings of the 2011 International Conference on Communication, Computing & Security*, 474-476.

ASHOK, J., RAJU, Y., MUNISHANKARAIAH, S. and SRINIVAS, K. (2010). STEGANOGRAPHY: AN OVERVIEW. *International Journal of Engineering Science*, 2.

Avcibas, I., Memon, N. and Sankur, B. (2003). Steganalysis using image quality metrics. *Image Processing, IEEE Transactions on*, 12(2), 221-229.

Barnes, J. (2011). A Survey of Recent Advances in Video Security.

Bender, W., Gruhl, D., Morimoto, N. and Lu, A. (1996). Techniques for data hiding. *IBM systems journal*, 35(3.4), 313-336.

Bhattacharyya, S. and Sanyal, G. (2012). A Robust Image Steganography using DWT Difference Modulation (DWTDM). *International Journal of Computer Network and Information Security (IJCNIS)*, 4(7), 27.

Chang, C. C., Chou, Y. C. and Lu, T. C. (2007). A semi-blind watermarking based on discrete wavelet transform. *Information and Communications Security*, 164-176.

Chen, W. J., Chang, C. C. and Le, T. (2010). High payload steganography mechanism using hybrid edge detector. *Expert Systems with Applications*, 37(4), 3292-3301.

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

Dumitrescu, S., Wu, X. and Wang, Z. (2003). Detection of LSB steganography via sample pair analysis. Proceedings of the 2003 *Information Hiding*, 355-372.

Goel, A., Gupta, R., Sahu, O. and Gupta, S. (2010). Improved digital watermarking techniques and data embedding in multimedia. *Department of CSE Singhania University, Rajasthan, Rupesh Gupta Department of Mechanical Engineering, Singhania University Rajasthan, OP Sahu Department of ECE, NIT Kurukshetra, Sheifali Gupta Department of ECE Singhania University, Rajasthan, India*.

Hamid, N., Yahya, A., Ahmad, R. B. and Al-Qershi, O. M. (2012). Image Steganography Techniques: An Overview. *International Journal of Computer Science and Security (IJCSS),* 6(3), 168.

Hopper, N. J. (2004). *Toward a theory of Steganography.* DTIC Document.

Horé, A. and Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. Proceedings of the 2010 *Pattern Recognition (ICPR), 2010 20th International Conference on*, 2366-2369.

Ji, L., Li, X., Yang, B. and Liu, Z. (2010). A further study on a PVD-based steganography. Proceedings of the 2010 *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, 686-690.

Johnson, N. F., Duric, Z., Jajodia, S. and Memon, N. (2001). Information hiding: steganography and watermarking—attacks and countermeasures. *Journal of Electronic Imaging*, 10(3), 825-826.

Juneja, M., Sandhu, P. S. and Walia, E. (2009). Application of LSB Based Steganographic Technique for 8-bit Color Images. *World Academy of Science, Engineering and Technology,* 50.

Kekre, H., Athawale, A. and Halarnkar, P. N. (2008). Increased Capacity of Information Hiding in LSBs Method for Text and Image. *International Journal of Electrical, Computer and Systems Engineering*, 2(4), 246-249.

Khalaf, E. T. and Sulaiman, N. (2011). A Robust Data Hiding Technique based on LSB Matching. *World Academy of Science, Engineering and Technology*, 58.

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

Luo, X., Liu, B. and Liu, F. (2005). Detecting LSB steganography based on dynamic masks. Proceedings of the 2005 *Intelligent Systems Design and Applications, 2005. ISDA'05. Proceedings. 5th International Conference on*, 251-255.

Mahajan, M. and Sharma, A. (2010). Steganography in Colored Images Using Information Reflector with 2^ k Correction. *International Journal of Computer Applications IJCA*, 1(1), 53-59.

Michaud, E. (2003). Current Steganography Tools and Methods.

Mohamed, M., Al-Afari, F. and Bamatraf, M. (2011). Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. *International Arab Journal of e-technology*, 2(1), 11-17.

Moler, C. (2011). Experiments with MATLAB: Chapter.

Morkel, T., Eloff, J. H. P. and Olivier, M. S. (2005). An overview of image steganography. Proceedings of the 2005 *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa*,

Nishikawa, K., Munadi, K. and Kiya, H. (2008). No-reference PSNR estimation for quality monitoring of motion JPEG2000 video over lossy packet networks. *Multimedia, IEEE Transactions on*, 10(4), 637-645.

Pan, F., Li, J. and Yang, X. (2011). Image steganography method based on PVD and modulus function. Proceedings of the 2011 *Electronics, Communications and Control (ICECC), 2011 International Conference on*, 282-284.

Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, 87(7), 1062-1078.

Picione, D. D. L., Battisti, F., Carli, M., Astola, J. and Egiazarian, K. (2006). A Fibonacci LSB data hiding tecnique.

Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. *Security & Privacy, IEEE*, 1(3), 32-44.

Ramkumar, M. and Akansu, A. N. (1999). Some design issues for robust data hiding systems. Proceedings of the 1999 *Signals, Systems, and Computers, 1999. Conference Record of the Thirty-Third Asilomar Conference on*, 1528-1532.

Raphael, A. J. and Sundaram, V. (2011). Cryptography and Steganography-A Survey. *International Journal*, 2.

Roque, J. J. and Minguet, J. M. (2009). SLSB: Improving the steganographic algorithm LSB. Proceedings of the 2009 *Proceedings The Ibero-American Congress on Information Security (CIBSI)*, 398-408.

Sharp, T. (2001). An implementation of key-based digital signal steganography. Proceedings of the 2001 *Information Hiding*, 13-26.

Shejul, A. A. and Kulkarni, U. L. (2011). A Secure Skin Tone based Steganography Using Wavelet Transform. *International Journal of Computer Theory and Engineering*, 3(1), 1793-8201.

Singh, N., Bhati, B. S. and Raw, R. (2012). DIGITAL IMAGE STEGANALYSIS FOR COMPUTER FORENSIC INVESTIGATION.

Wang, H. and Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, 47(10), 76-82.

Westfeld, A. and Pfitzmann, A. (2000). Attacks on steganographic systems-breaking the steganographic utilities ezstego. Proceedings of the 2000 *Jsteg, Steganos, and S-Tools-and Some Lessons Learned," Lecture Notes in Computer Science*,

Wolak, C. M. (2000). Digital Watermarking. *Preliminary Proposal, Nova Southeastern University, United States*.

Wu, H. C., Wu, N. I., Tsai, C. S. and Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. Proceedings of the 2005 *Vision, Image and Signal Processing, IEE Proceedings-*, 611-615.

Xiu-ying, M. and Jia-jun, L. (2009). HVS-Based Imperceptibility Evaluation for Steganography. *Scalable Information Systems*, 152-161.

Zhang, X. and Wang, S. (2005). Steganography using multiple-base notational system and human vision sensitivity. *Signal Processing Letters, IEEE*, 12(1), 67-70.