STEGANOGRAPHY BASED ON UTILIZING MORE SURROUNDING PIXELS

MASOUD AFRAKHTEH

UNIVERSITI TEKNOLOGI MALAYSIA

STEGANOGRAPHY BASED ON UTILIZING MORE SURROUNDING PIXELS

MASOUD AFRAKHTEH

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

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

MARCH 2010

ABSTRACT

The purpose of this study is to investigate the application of least significant bit insertion method (LSB) in concealing a definite amount of message bits inside a typical media such as an 8-bit gray-scale image and develop an alternative model structure selection algorithm based on considering more surrounding pixels in order to compute the best capacity value for each target pixel. Conventional LSB method's concept is used as the benchmark for the proposed algorithms. A model structure selection based on not choosing selected pixels as immediate neighbors of the target pixel is proposed in this study to reduce image's distortion made by embedding random bits or in other words to get a higher imperceptibility. The imperceptibility measures used for evaluation are called peak signal to noise ratio (PSNR), Watson metric and Universal quality index (Q). Previous algorithms utilize at most four (4) out of eight (8) surrounding pixels as multiple based notational system (MBNS) uses three (3) pixels. The effect of considering the rest of surrounding pixels on the performance of the developed model is studied and the effectiveness and shortcomings are highlighted. Results are compared between MBNS, Adaptive and Fixed methods. It is discovered that with similar number of payloads, in most cases, the proposed methods perform better than MBNS in terms of exploring better imperceptibility in predicting more accurate capacity of each target pixel. In addition, the use of pseudo random numbers generator (PRNG) considered for finding the walk path through the image using a stego key and a seed number to provide needed security. Furthermore, the method is proved to be robust against one of the common attacks to stego-images known as Chi-squared attack.

ABSTRAK

Tujuan kajian ini adalah untuk mengenalpasti kaedah penyisipan bit yang paling sedikit dalam menyembunyikan jumlah sebenar bit mesej dalam satu media khas seperti 8 bit imej hitam putih dan membangunkan alternatif model struktur pemilihan algoritma, berdasarkan pixel disekitarnya dengan tujuan mengira keupayaan yang terbaik untuk setiap sasaran pixel. Kaedah penyisipan bit yang lama digunakan sebagai tanda untuk algoritma yang dicadangkan. Satu pilihan struktur model berdasarkan pixel yang tidak terpilih sebagai jiran segera bagi piksel sasaran dicadangkan dalam kajian ini untuk mengurangkan herotan imej dibuat dengan membenamkan bit secara rawak atau dengan kata lain untuk mendapatkan penerimaan yang lebih baik. Isyarat puncak untuk nisbah kebisingan atau *Peak signal to noise ratio (PSNR),* Matriks Watson dan indeks kualiti sejagat digunakan untuk menilai ukuran penerimaan. Algoritma sebelum ini menggunakan empat daripada lapan piksel sekitar sebagai MBNS yang menggunakan tiga piksel. Kesan daripada menganggap lebihan piksel dalam prestasi untuk pembangunan model telah dikaji dan keberkesanan serta kekurangan dikenalpasti. Hasil kajian dibandingkan antara kaedah MBNS, Adaptif dan mod tetap. Dengan menggunakan nombor yang serupa, dalam kebanyakan kes, kaedah yang dicadangkan adalah lebih baik berbanding dengan MBNS bagi ukuran penerimaan dalam meramal keupayaan lebih tepat bagi setiap piksel sasaran. Selain itu, penggunaan *pseudo random numbers generator (PRNG)* adalah untuk mencari laluan gambar menggunakan kekunci stego dan jumlah benih untuk menyediakan keselamatan yang diperlukan. Tambahan pula, kaedah ini telah terbukti yang paling kukuh bagi serangan umum kepada *stego-images* yang dikenali sebagai serangan *Chi-squared*.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

Since the early days, individuals send messages as a form of communication. In some situations, it was supposed to be sent by means of a pre-secured method hoping that no other person except the desired receiver could get the meaning of the content. So, people always hide their favorite messages by a variety of methods (Kahn, 1967; Norman, 1973). For instance, ancient Greeks put the message on the underlying wood of a tablet and then covered it with some wax to be considered as a kind of useless thing. Another method is that a messenger shaved the head and wrote something on his head. After his hair grew back, he was sent to somewhere and nobody could ever detect or guess that if he had any message embedded on his head (Kahn, 1967). Another secure method is to use invisible inks and it was widely used in World War II (Kahn, 1967). With invisible ink, a seemingly innocent letter could include another written message between the lines (Zim, 1948). In addition, there were some innovative methods to transfer these secret messages by means of an ordinary message, like what a German spy did in World War II. He transferred null-cipher message that included one sentence. The receiver could extract the second

letters of each word to find another sentence. The secret message was the statement: "Pershing sails from NY June 1". Here is the long cover message sent: "*Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.*" (Kahn, 1967)

In comparison with today's technologies, lots of new interesting methods are appeared and computers play the most important role in this section. It is worth mentioning that a great deal of information hiding systems deal with media files such as video, sound and different types of images formats. So, digital media can be transmitted over networks. A secured transmission is mostly wanted in such an area in order to protect secret messages. There is an art called Steganography that is in relation with hiding the secret data in a media like an image so that it does not attract any attention and looks like an innocent medium.

1.2 Problem Background

There are lots of algorithms used in image steganography area. However, they have their own weaknesses and strengths. Since Least Significant Bit (LSB) insertion method is one of the simplest data hiding techniques, it has long been a focus for researchers to propose attacking methods and they are called either steganalytic or steganalysis attacks. The advantage of LSB steganographic data embedding is that its understanding is simple and it can be easily implemented. However, it is proved that sometimes it is not secure at all (Lee *et al*., 2009) because some harmful statistics are exploited that reveal the existence of the secret data. These harmful statistics are image's distortion and observing some pair of values created after embedding process. If there is any method that is able to decrease the existence of these factors then imperceptibility is improved. In this study most of the

effort is done to get a better imperceptibility by removing PoVs and decreasing image's distortion.

1.2.1 Image's Distortion Problem

The conventional LSB insertion method just embeds an amount of message bits inside a pre-defined number of LSBs of the cover-image regardless of the variation of colors around the target pixel. It means that it does not consider human vision system and the very first goal is how to embed more in the image. That is why conventional LSB method embeds the biggest amount of secret bits. Another method which is identical to LSB method is called Optimal method that uses an adjustment technique to decrease the error made after embedment. This is one kind of creating distortion by changing pixels LSBs by random bit values.

The method called as an adaptive image steganography model based on minimum-error LSB replacement (Lee and Chen, 1999) takes off the restriction of fixed embedding size in each pixel. It reduces the embedding error and provides higher embedding capacity. However, it is limited to use just four (4) closest neighbors rather than utilizing all eight (8) neighbors (three neighbors on the top and one on the left). This fact leads to see some more cumulative distortion as the embedding process proceeds from the top left-most point to the bottom right-most point of the image. Each new pixel's gray value is updated by the modified values made in the prior steps and it makes what is called cumulative image's distortion. In addition, unlike optimal LSB method that exploits all LSBs of a gray-scale image, this method loses some portion of capacity to achieve more image quality based on human vision sensitivity (HVS).

Another method named EZ-stego uses a color pallet to find the closest color (two adjacent colors) in the predefined pallet. Although it uses adjacent colors, it is easily attacked by a visual attack like substituting all even pallet colors' values with black and odd numbers with white or vice versa. Therefore, the distortion is shown by a filtering method (Figures 1.1, 1.2). The usefulness of this attack is limited to the texture of the original image, and it does not work out on a kind of flooring tile image (Figure 1.3).

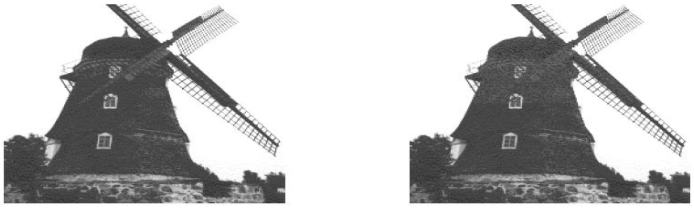

Figure 1. 1 Windmill as original image on the left, and embedded image on the right (Westfeld and Pfitzmann, 2000).

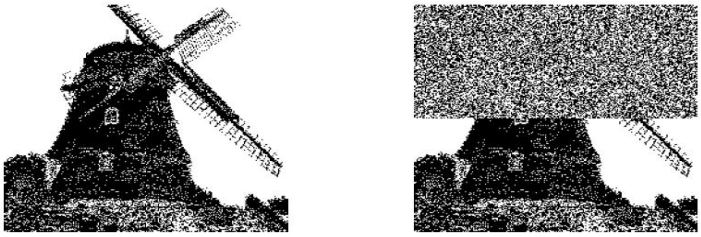

Figure 1. 2 Filtered image of Figure 1.1, nothing embedded (Left) and 50% capacity is embedded on the right image (Westfeld and Pfitzmann, 2000).

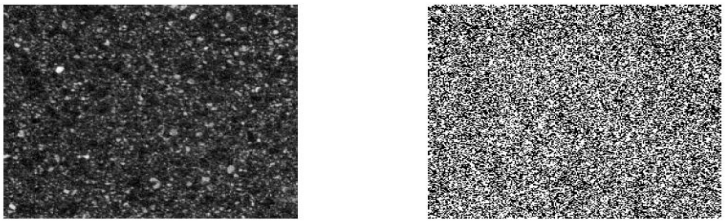

Figure 1. 3 A flooring tile as cover media on the left and its filtered image on the right (Westfeld and Pfitzmann, 2000).

1.2.2 Pair of Values Problem (PoVs)

Another method (Zhang and Wang, 2005) also presented an adaptive steganographic scheme with the multiple-based notational system (MBNS) based on human vision sensitivity (HVS). The hiding capacity of each image pixel is determined by its local variation. The formula for computing the local variation takes the human visual sensitivity into account. A great local variation value indicates that the area to where the pixel belongs is either a busy or edge area. It means more secret data is hidden. This way, the stego-image's quality degradation is so much invisible to the human eye. However, the sequential processing mode of the pixel values increases the cumulative distortion and it also leads to see some pair of values created in the histogram of the stego-image (Figure 1.4). Pair of values are made as the algorithm fits random bits in LSBs of pixels (the same frequency of gray-scale values in image's histogram for all 2k and 2k+1 values). Therefore, assuming that number of 0s and 1s are approximately identical, when the algorithm embeds some bit(s) inside each pixel, with the probability of 50 percent, the least significant bit value is either zero or one. The idea of the existence of PoVs is similar to the theoretic analysis of PoVs (Lee *et al.*, 2009). In both methods, just LSB causes PoVs. If all k-bits are substituted, the LSB is again changed by chance of 50 percent and makes a pair of value. Ultimately, this is useable for steganalyzers in order to detect the existence of the message (such as chi-squared attack).

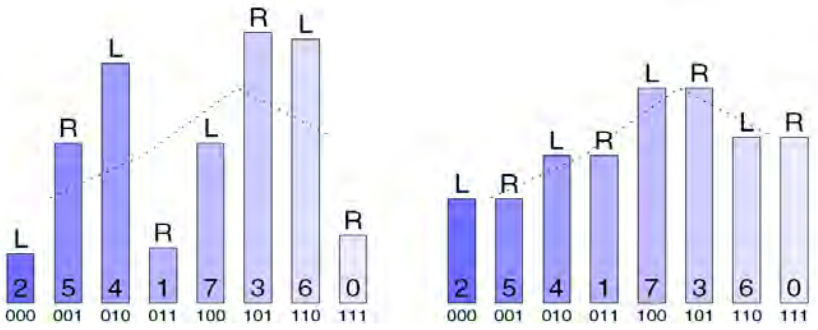

Figure 1. 4 PoVs artifact exists in the histogram after applying LSB embedding (Westfeld and Pfitzmann, 2000).

1.2.3 Summary

Often steganographic schemes create regular statistical evidence that is used to detect the secret message with respect to image quality properties (Avcibas *et al*., 2003). One example is the detection of secret message existence in the LSB of natural continuous-tone images (Dumitrescu *et al., 2002*). The key to this success is based on finding a group of pixels that their corresponding cardinalities are changed with LSB method as the message bits are scattered randomly not sequentially. All steganalysis methods take advantage of the measures such as existence of image's distortion, and PoVs that give consistent scores across an image class. From this point of view, it results in a visual attack that uses multivariate regression on the selected quality metrics (Avcibas *et al.*, 2001). Ultimately, once the natural LSBs are changed with random bits in smooth areas, then it is easily detected by means of evidences left.

There is just one important factor which makes steganalysis harder and that is when imperceptibility rises. If a new method proposes some way that guarantees achieving an acceptable imperceptibility as well as removing PoVs, it is regarded as a robust algorithm to such visual attacks as chi-squared attack.

1.3 Problem Statement

The principle goal of steganography is to cover the weaknesses such as statistical anomalies of a stego-image's distortion and existence of PoVs that is exploited by steganalysis methods. One method uses a probabilistic embedding so as to decrease the changes made by LSB insertion (Lee and Chen, 1999). Another

method chooses its proper pixels having the least likely risk of being attacked and detected by Steganalyzers (Provos, 2001). In other words, there is a need to choose the best pixels unlike the conventional LSB insertion method that chooses the target bits sequentially. Furthermore, in order to add more security, the message can be compressed and then encoded by a secret key to be embedded in the cover image (Figure 1.5). The reverse mode is not recommended since number of compression methods are limited so that the probability of being attacked goes higher. Because some content-dependent patterns in the original message exposes the message existence. Thus the way these characteristics are concealed is so much important (Lee, 1999). But, in this study the focus is more on the algorithm such that these issues are ignored however they are needed for guaranteeing more security. In this study, an algorithm is proposed based on the following ideas:

- Choosing **some** pixels of a typical gray-scale image with **more capacity**, considering **a probability value** for each target pixel. The idea is based on the algorithm offered by Lee *et al.* (1999). This is just due to scattering message bits, in order not to be detected easily.
- Removing the statistical regular patterns (PoVs) with help of an advanced technique which is **incrementing or decrementing** the pixel value instead of just flipping LSBs with desired message bits (Lee *et al.* ,2009).
- Using **local variation formula** (considering human vision sensitivity-HVS) to determine **the best capacity** of each pixel with respect to each pixel's adjacent neighbors (Zhang and Wang, 2005).
- Choosing **more adjacent neighbors** so as to decrease the cumulative distortion (more than 3 neighbors and perhaps all eight neighbors).

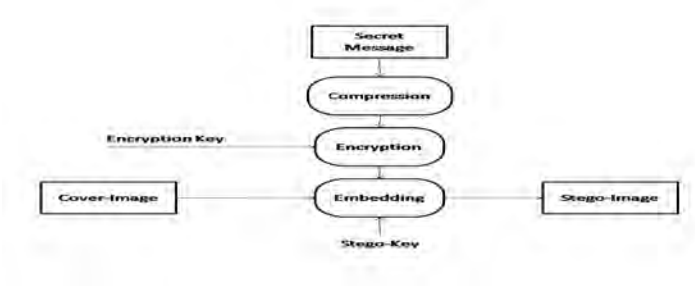

Figure 1. 5 The process of message encoding and message extracting

A hybrid method of all named methods assures that there will be no existence of any PoVs. Therefore, the following questions are answered in this study:

1. How to choose the desired pixels non-sequentially?
2. Which policy will perform better so as to get the maximum image's imperceptibility and provide lesser cumulative image's distortion rather than maximum capacity?
3. How to remove regular patterns (PoVs)?

1.4 Objectives

The major goals in this study are as follows:

1. To design a steganography algorithm that increases **imperceptibility.**
2. To get the same acceptable **payload or capacity** as MBNS method does.
3. To **add** and **analyze the security** against chi-squared attack.

These goals are fulfilled as follows:

1. The more surrounding pixels, the more imperceptibility. These pixels are considered in local variation formula. In this way more accurate number is estimated for each target pixel. Image's distortion decreases a great deal when other surrounding pixels' values are used and vice versa.
2. Several payloads are checked under the same conditions for either of the methods.
3. The desired security is provided by considering two keys namely stego key and seed number. Seed number is used to embed secret bits in the embedding area and the stego key is used to embed secret info including seed number in the secret area which is located in the first column and row of the cover image. To analyze security by chi-squared attack a

technique named as adjustment technique is utilized that makes chi-squared attack unable to find any PoVs.

1.5 Project Scope

In this study, the scope of the proposed algorithm is mainly based on below items:

1. The desired file expected to be embedded (secret data) is the ordinary text file format.
2. The desired media for hiding the text file (cover media) is an 8-bits gray-scale image file format.
3. The proposed method uses the basic concept of LSB insertion method.
4. There are two keys used in the proposed algorithm (stego-key and seed number) but finding the best key is ignored in this study.
5. Chi-squared attack is the desired visual attack in order to prove the effectiveness of the proposed algorithm.
6. The visual language used for coding is MATLAB.
7. The standard images for testing purposes are *Lena, Man and Finstones* .

1.6 Importance of the Research

The enormous increasing growth rate of internet applications and wide usage of websites is about to look so unsafe that it needs much more security. As a result,

REFERENCES

Anderson, R.J. and Petitcolas, F.A.P. (May 1998). On the limits of Steganography. *IEEE Journal of selected Areas in Communications.*

Aura, T. (1995). Invisible Communication. *EET technical report*. Finland: Helsinki Univ. of Technology.

Avcibas, I., Avcıbas, I., Sankur, B., Akarun, L., Anarim, E., Memon, N. and Yemez, Y. (2001). *Image Quality Statistics and Their Use in Steganalysis and Compression.* Doctor of Philosophy. Institute for Graduate Studies in Science and Engineering.

Avcibas, I., Memon, N. and Sankur B. (2003). Steganalysis Using Image Quality Metrics. *IEEE transactions on Image Processing*. IEEE, 12, 221-229.

Brin, S., Davis, J. and Garcia-Molina, H. (1995). Copy Detection Mechanisms for Digital Documents. *Proceedings of the ACM SIGMOD Annual Conference*. San Jose.

Broder, A.Z. (1993). Some applications of Rabin's fingerprinting method. *Methods in Communications, Security, and Computer Science.* London: Springer-Verlag, 143-152.

Broder, A.Z. (1998). On the Resemblance and Containment of Documents. *Proceedings of Compression and Complexity of Sequences 1997*. IEEE Computer Society, 21-27.

Chan, C.K. and Cheng, L.M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition.* Vol. 37 (No. 3), 469–474.

Clair, B. (2001). *Steganography: How to Send a Secret Message.* Saint Louis University.

Currie, D.L. and Irvine, C.E. (1996). Surmounting the effects of lossy compression on Steganography. *19th National Information Systems Security Conference.*

Dumitrescu, S., Wu, X. and Memon, N. (2002). Steganalysis of Random lsb Embedding in Continuous-tone Images. *IEEE International Conference on Image Processing*.

Fan, L., Cao, P., Almeida, J. and Broder, A. (2000). Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol. *IEEE/ACM Transactions on Networking*. Vol. 8 (No. 3).

Fridrich, J., Goljan, M. and Du, R. (2001). Reliable Detection of LSB Steganography in Color and Grayscale Images. *IEEE Multimedia*. 8, 22-28.

Fridrich, J. and Goljan, M. (2002). Practical Steganalysis of Digital Images-State of the Art. *In Proceedings of SPIE*. 1-13.

Fridrich, J., Goljan, M. and Soukal, D. (2003). Higher-order statistical steganalysis of palette images. *Security and Watermarking of Multimedia Contents*. Proc. SPIE 5020,178–190.

Isbell, R.A. (2002). Steganography: Hidden Menace or Hidden Savoir. *Steganography White Paper*.

Johnson, N. F, Jajodia, S. and Mason, G. (1998). Exploring Steganography: Seeing the Unseen. *IEEE Computer*. 31, 26-34.

Kahn, D. (1967). *The Code breakers*. ISBN 0-684-83130-9. New York: Macmillan.

Lee, Y.K. and Chen, L. h. (1999). An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement. *In Proceedings of the Ninth National Conference on Information Security*. 14-15. Taichung, Taiwan, 8-15.

Lee, K., Westfeld, A., Lee, S. and Technische Universität esden (2006). Category Attack for LSB Steganalysis of JPEG images. *Digital Watermarking (5th International Workshop)*. London: Springer-Verlag, 35-48.

Lee, Y.K., Bell, G., Huang, S.Y., Wang, R.Z. and Shyu, S.J. (2009). An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding. *Advances in Image and Video Technology*. Berlin / Heidelberg: Springer, 349-360.

Manber, U. (1994). Finding Similar Files in a Large File System. *Proceedings of the USENIX Winter Technical Conf.*

Mayache, A., Eude, T., and Cheri, H. (1998). A comparison of image quality models and metrics based on human visual sensitivity. *Proc. Int. Conf. Image Processing (ICIP'98)*. vol. 3, Chicago, IL, 409–413.