International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.6 (2015), pp.195-202
http://dx.doi.org/10.14257/ijmue.2015.10.6.20

A New Model for Hiding Text in an Image Using Logical Connective

Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda and Mustafa Mamat

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Tembila Campus,Terengganu, Malaysia
sitidhalila@unisza.edu.my

Abstract

The objective of this study is to propose a new model for hiding text in an image. The proposed model use logical connective in propositional logic to calculate a new binary number of secret message. This model can produce a low computational complexity of steganography because of the simplicity of the proposed algorithm. Moreover, the using of simple operator but very efficient is expected to be able to hide high capacity of a secret message.

Keywords: *Steganography, Image, Least Significant Bit (LSB), Logical Connective*

1. Introduction

Steganography has been progressively becoming one of a popular technique to be used for secret communication between two parties or more. The term of steganography originated from two Greek words which were stegano and graphos. Stegano could be described as cover or secret and graphos defined the meaning of writing or drawing. The combination of both words delineated the meaning of "covered writing" [1]. History of steganography could be traced since thousand years ago. During those years, body parts had been used as a medium to transmit a secret message by using invisible ink, tiny punctures on chosen characters, hidden tattoos and microdots [2].

The main objective of steganography is to transfer the information securely. Steganography is a technique that could be used to conceal confidential information into an object or carrier so that unintended recipient does not notice the existence of a secret message. According to the authors [3], over the years, several steganography methods began to propose embedded secret message in multimedia objects such as images. Images could be a powerful host to hide information because the spacious spaces it offers. Moreover, the changed in digital images are usually unnoticeable to naked eye. Nowadays, computer technology has given a new life to the ancient steganography. Computer technology introduces digital steganography and makes the steganography easier to execute but harder to crack. These facts motivate this study to be conducted and to propose a new model for hiding text in image.

2. Overview of Steganography

Steganography could be described as a practice of hiding data within an object. The authors [4] defined that steganography as the art of transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data. The main objective of steganography was to provide a secure communication in a completely undetectable manner and also aimed to avoid suspicious from unintended recipient about the transmission of data [5].

ISSN: 1975-0080 IJMUE

The authors [6] stressed that in steganography there were three requirements that researcher needed to pay attention when designing any steganography algorithm. The three requirements were capacity, robustness and invisibility. Capacity was the amount of a secret message that could be embedded in a cover image. Robustness ensured that a stego-object preserved the information inside it even though it went through some reprocessing operation. However, there was a tradeoff between capacity and robustness. When the capacity of the secret message was high then the robustness of the stego-object would become low. A little changed to the stego-object would destroy information completely. Invisibility was referred to a situation whereby the embedded data could not be traced or there were no signs that the steganography had been used to the image. The visibility was directly influenced by the size of the secret message, the format and the content of the carrier.

3. General Concept of Steganography

Steganography can be achieved when the user can retrieve a secret message unnoticeably. This involves two main processes. The first process is embedding process, where in this process; a secret message is embedded in the host. The host and a secret message can be an image, a video, an audio or text. The second process is involving the extraction of the secret message that has been embedded.

Generally steganography concepts can be represented by a basic model of steganography as in Figure 1. The basic model of steganography consists of the following terms in Table 1.

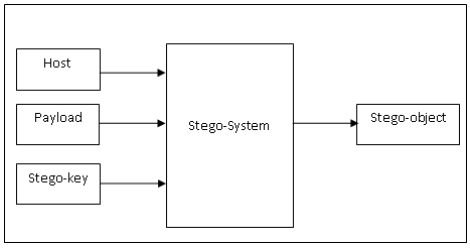

Figure 1. The Basic Model of Steganography [7]

Table 1. Term Definition of Steganography Model [7]

Term	Description
Payload	refers to the information that the sender concern to keep it confidential. The payload can be plain text, cipher text, audio, image or anything that can be embedded in a bit stream such as a copy right mark or a serial number
Stego-key	is also called a password. It is an optional choice whether the sender wants to use the stego-key or not. However, when using stego-key, the sender can ensure that only the recipient with the right key can extract the secret message back
Host	also refers as cover object that used to embed secret message into it. Cover-object can be a text, image or audio and also html pages
Stego-object	is a host with the embedded secret message after having some computational calculation based on formula
Stego-system	is a formula that converts host with the payload to the stego –object

4. Image Steganography

Recently, image has been used in steganography as a carrier to transmit or send the secret message from a sender to a receiver. Image steganography has attracted extensive researches compared to other types of steganography. The reason image has been used frequently in steganography is because a huge amount of information can be hidden without noticeable impact to the image that is used as carrier. In addition, the usage of image in information hiding is an ideal technique to have a secured steganography because digital image is insensitive to human visual system [8].

In a computer, an image is represented in an array of numbers that represents the light intensities at various points. Most images contain a rectangular map called pixel which represent a bit of the image. The pixels are displayed horizontally row by row [9-10]. Digital image is typically stored in 8-Bit file or 24-Bit file. According to the authors [11], an 8-bit is the smallest bit depth in the current scheme, meaning that for each pixel, the bit used is 8. The image that used 8-bits are monochrome and grayscale image. In a 24-bit image, there is more space that can be manipulated to hide the secret message. In this file image, there are three primary colour; Red, Green and Blue. Each colour represents 1 byte and this image used 3 bytes per pixel to present the colour value.

According to the authors [12], image steganography techniques can be identified into four basic categories as follows:

a) Substitution technique involves replacing redundant bits in the cover image with the bits from the secret message such as Least Significant Bit (LSB) technique
b) Statistical technique means embedding only one bit of information in a digital carrier, and creating a statistical change. For example, Pseudorandom Permutations (PP) technique
c) Transform domain technique involves hiding message data in a signal. Example of transform domain technique is Discrete Cosine Transform (DCT).
d) Spread spectrum technique is the technique of dividing transmitted information into small pieces

5. Least Significant Bit

From image steganography techniques as mentioned in Section 4, this proposed model shall focus on substitution technique specifically Least Significant Bit (LSB) technique. LSB refers to the right most bit in a binary integer where LSB replaces the lowest bits in images with secret message bits. LSB is the common and simple approach for hiding information. This algorithm provides a high embedding capacity, high quality and low computational complexity of steganography. LSB in an image is said to have a high capacity of embedding secret message because many pixel value of images can be manipulated and replaced with the secret message [13-14].

The authors [15] proposed a steganography technique to embed a secret data inside a cover image based on LSB replacement method. The embedding process involved distributing the secret message inside a shared colored image. The uniqueness of the data distribution process, made this technique resistant to the attacks as it was difficult for the attackers to reconstruct the shape from stego-images. Additionally the authors claimed that this method created a good peak-signal-to-noise ratio (PSNR) value.

The authors [16] discussed about steganography methods for sharing secret message by using multicover adaptive steganography. In this method, the secret message was embedded into LSB plane and 2LSB plane of the cover image. This method applied XOR and AND operators to the secret message bit and the image. The author evaluated the performance of proposed method by calculating the PSNR and structural similarity (SSIM) index. From the experimental results, the author concluded that the proposed

methods fulfil following requirements; high quality shares, lossless reconstruction and computational efficiency at the same time.

The authors proposed a new technique to enhance the security and the quality of the image steganography that based on LSB. The technique implemented a variation of plain LSB algorithm by using bit inversion method. The advantages of the technique were to reduce the number of modified bits, produced a high quality of stego-image and enhance the image quality and robustness [17].

A research presented by Akhtar et al. [18] proposed an improvement of plain LSB by using bit inversion technique. These LSB inversion method was proved could be used to increase the quality of final image. The authors discussed that less number of pixels were modified if compared to plain LSB method and eventually lead to enhancement of PSNR in stego-image. The advantages of this inverted LSB scheme was the difficulty to recover the message because some of the LSBs had been inverted.

6. The Steganography Connective Model

This study proposes a Steganography Connective Model (SCM) using propositional logic. A propositional logic describes the declarative sentence that is either true or false but not both. The new proposition from two or more propositions is form by using connective logical (CL) [19].

Figure 2 shows the SCM. The CL is used as an algorithm to calculate a new binary number of secret messages while the most significant bit (MSB) of each pixel is used as a key. MSB is a first bit of each pixel and it has a great significant value. Generally, the MSB of each pixel calculated with secret message using operator Negation, OR and XOR to produce a new secret message. This new secret message will be embedded in the LSB of each pixel.

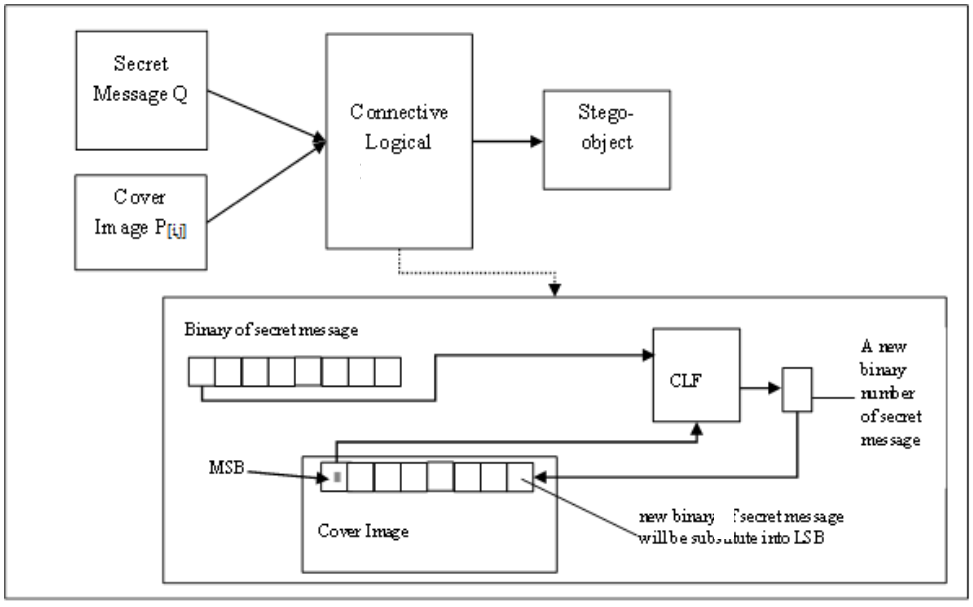

Figure 2. Steganography Connective Model (SCM)

CL algorithms consist of these equations:

$R1\ [i,j] = \neg P[i,j]$ (eq. 1)

$R2\ [i,j] = R1[i,j]\ V\ Q$ (eq. 2)

$R3\ [i,j] = R2[i,j] \oplus Q$ (eq. 3)

$R4\ [i,j] = R3[i,j]$ (eq. 4)

Definition of each variable is:

P is MSB of pixel
i and j is coordinate of each pixel, i=0, 1, 2, …, n; j=0, 1, 2, …, n
Q is a binary of the secret message
S is the LSB of pixel

Algorithm for Embedding

The proposed model manipulates CL as an algorithm for embedding process. This embedding process is done on the sender side. After the embedding process completed, the sender sends the stego-image to the receiver. The complete algorithm for embedding is shown as below.

Input: An image to use as carrier, the secret message
Output: A stego-image containing the secret message
The steps are as follows:

1. The image and the secret message each is converted into its binary number.
2. The length of the binary number for image and secret message are compared.
3. If the lengths of cover image are more than secret message, step 4 is performed, else end the process.
4. Perform calculation to the secret message with the most significant bit of pixel image.
5. The result from step 4 is replaced to the least significant bit of the each pixel image.
6. Repeat the steps until all the secret bit value are replaced.
7. End the process.

7. Implementation of SCM

The following example explain logical connective algorithm. The authors used ‘buku’ as a secret message and choose an image as a cover object.

1. Choose a cover image
2. Convert the cover image to binary number
3. Insert a secret message. Let say the secret message is ‘buku’
4. Convert the secret message to binary number. The binary number for each letter of ‘b’, ‘u’, ‘k’, ‘u’ as:
   b: 01100010
   u: 01110101
   k: 01101011
   u: 01110101
5. Perform calculation using eq. 1, eq.2 and eq. 3 on binary number of the secret message, M_i. The MSB for Pixel [0,0], P is being calculated using negation operator which represented by R1. Then, R1 is used to calculate with secret message, Q by using OR operator, producing R2. The new secret message, R3 is produced by calculating R2 with Q using operator XOR. The result of each equations are shown in Table 2.

Table 2. Result of Calculation Process for Equation

M_i	$Pixel_{[i,j]}$	P	Q	R1= ¬P	R2= R1 V Q	R3= R2 ⊕ Q
	0,0	0	0	1	1	1
	1,0	1	1	0	1	0

	2,0	0	1	1	1	0
B	3,0	1	0	0	0	0
	4,0	0	0	1	1	1
	5,0	1	0	0	0	0
	6,0	0	1	1	1	0
	0,1	1	0	0	0	0
	1,1	0	0	1	1	1
	2,1	1	1	0	1	0
u	3,1	0	1	1	1	0
	4,1	1	1	0	1	0
	5,1	1	0	0	0	0
	6,1	1	1	0	1	0
	0,2	0	0	1	1	1
	1,2	0	1	1	1	0
	2,2	0	0	1	1	0
	3,2	1	1	0	1	0
k	4,2	0	1	1	1	0
	5,2	0	0	1	1	1
	6,2	1	1	0	1	0
	0,3	0	0	1	1	1
	1,3	1	1	0	1	0
	2,3	1	1	0	1	0
	3,3	0	0	1	1	1
	4,3	1	1	0	1	0
	5,3	0	1	1	1	0
u	6,3	1	1	0	1	0
	0,4	1	0	0	0	0
	1,4	1	1	0	1	0
	2,4	0	0	1	1	1
	3,4	0	1	1	1	0

6. Then substitute $R3_i$ into S_i. The results after the substitution are shown as below.

Table 2.1 Pixel Value of Image Before Substitution Process

i, j	0	1	2	3	4	5	6
0	01010101	10101010	01101010	10110010	00110101	11100010	00110110
1	11101010	00010101	10110010	00100110	11100010	10110110	10101010
2	01010101	00101010	01101010	10110010	00110100	01101011	11010111
3	00101010	11010101	10110010	00010110	10100110	00110010	10101010
4	11110101	10101010	01101011	00110010			

Table 2.2 Pixel Value of the Image After Substitution Process

i, j	0	1	2	3	4	5	6
0	01010101	10101010	01101010	10110010	00110101	11100010	00110110
1	11101010	00010101	10110010	00100110	11100010	10110110	10101010
2	01010101	00101010	01101010	10110010	00110100	01101011	11010110
3	00101011	11010100	10110010	00010111	10100110	00110010	10101010
4	11110100	10101010	01101011	00110010			

7. Conclusion

This paper proposed a simple and an efficient model for calculating secret message that can be embed in an image. This proposed model used Connective Logical (CL) as an algorithm to calculate a new binary number of secret messages while the most significant bit (MSB) of each pixel was used as a key. MSB was a first bit of each pixel and it has a great significant value. Generally the MSB of each pixel calculated with secret message using operator Negation, OR and XOR to produce a new secret message. This new secret message would be embedded in the LSB of pixel. The implementation of this model can produce a low computational complexity of steganography because of the simplicity of the proposed algorithm.

Acknowledgements

This research is fully sponsored by Centre of Research Innovation & Management (CRIM), Universiti Sultan Zainal Abidin (UniSZA), Malaysia. Project No is UniSZA/14/GU (021).

References

[1] V. Sharma and S. Kumar, "A New Approach to Hide Text in Images Using Steganography," International Journal of Advanced Research in Computer Science and Software Engineering. vol. 3 no. 4, **(2013)**.
[2] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," Signal Processing, vol. 90 no. 3, **(2010)**.
[3] V. L. Reddy, A. Subramanyam and P.C Reddy, "Implementation of LSB Steganography and Its Evaluation for Various File Formats," Int. J. Advanced Networking and Applications, vol. 2 no. 5, **(2011)**.
[4] G. Abboud, J. Marean and R.V. Yampolskiy, "Editors. Steganography and Visual Cryptography," Proceedings of Computer Forensics in Systematic Approaches to Digital Forensic Engineering (SADFE), CA, May 20 **(2010)**.
[5] M. Y. Wu, Y. K. Ho and J. H. Lee, "An Iterative Method of Palette-Based Image Steganography," Pattern Recognition Letters. vol. 25 no. 3 **(2004)**.
[6] M. S. Subhedar and V. H. Mankar, "Current Status and Key Issues in Image Steganography," A Survey. Computer Science Review, vol. 3, **(2014)**.
[7] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin and M. Z. I. Shamsuddin, "Editors. Information Hiding Using Steganography," Proceedings of Telecommunication Technology Proceedings, January 14-15 **(2003)**.
[8] C. Maiti, D. Baksi, I. Zamider, P. Gorai and D. R. Kisku, "Data Hiding in Images Using Some Efficient Steganography Techniques," Signal Processing, Image Processing and Pattern Recognition, **(2011)**.
[9] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen Computer," vol. 31 no. 2 **(1998)**.
[10] M. S. Rana, B. S. Sangwan and J. Jangir, "Art of Hiding: An Introduction to Steganography," International Journal of Engineering and Computer Science, vol. 1 no. 1, **(2014)**.
[11] S. Singh and G. Agarwal, "Use of Image to Secure Text Message with the Help of LSB Replacement," International Journal of Applied Engineering Research. 1 **(2010)**.
[12] A. H. Lashkari, A. A. Manaf, M. Masrom and S. M. Daud, "A Survey On Image Steganography Algorithms and Evaluation," Digital Information Processing and Communications, **(2011)**.
[13] M. Tang, J. Hu and W. Song, "A High Capacity Image Steganography Using Multi-Layer Embedding," Optik-International Journal for Light and Electron Optics, vol. 125 no. 15, **(2014)**.
[14] S. Sarreshtedari and M. A. Akhaee, "One-Third Probability Embedding: A New ±1 Histogram Compensating Image Least Significant Bit Steganography Scheme," IET Image Processing, vol. 8 no. 2, **(2013)**.
[15] K. A. Darabkh, I. F. Jafar, R. Al-Zubi and M. Hawa, "Editors. An Improved Image Least Significant Bit Replacement Method," Proceedings of International Convention on Information and Communication Technology, Opatija, May 26-30 **(2014)**.
[16] H. D. Yuan, "Secret sharing with multi-cover adaptive steganography," Information Sciences, vol. 254, **(2014)**.
[17] N. Akhtar, S. Khan and P. Johri, "Editors. Enhancing the Security and Quality of LSB Based Image Steganography," Proceedings of International Conference on Computational Intelligence and Communication Networks, Mathura**,** September 27-29 **(2013)**.

[18] N. Akhtar, S. Khan and P. Johri, "Editors. An Improved Inverted LSB Image Steganography," Proceedings of International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad**,** February 7-8 **(2014)**.
[19] K. H. Rosen, "Editor, Discrete Mathematics and its Applications," New York: Mc Graw Hill, **(2007)**.

Authors

Siti Dhalila Mohd Satar, she is currently works as a lecturer at Faculty of Informatics and Computing, University Sultan Zainal Abidin, Terengganu. She holds a B.S. degree in Information Technology from University Kebangsaan Malaysia (UKM), in 2008 and MSc in Computer Science (Information Security) from University Teknologi Malaysia (UTM), Malaysia. Her research interests are Information Security, and Information Quality

Nazirah Abd Hamid, she s a lecturer in University Sultan Zainal Abidin, Terengganu. She holds a degree in Bachelor of Information Technology from University Utara Malaysia (UUM), in 2004 and M. Sc. Com. (Information Security) from University Teknologi Malaysia (UTM), Malaysia. Her research interests are Information Security and Human Computer Interaction (HCI).

Fatimah Ghazali, she is a lecturer at Faculty of Informatics and Computing, University Sultan Zainal Abidin, Terengganu. She is graduated from University Kebangsaan Malaysia (UKM) in 1999 with B.S. degree in Information Technology and MSc in Computer Science (Software Engineering) from University Putra Malaysia (UPM), Malaysia. Her research interests are Software Engineering and Security and Information Quality

Roslinda Muda, she is graduated in Master of Computer Science (Information Security) and Bachelor of Science (Computer) from Universiti Teknologi Malaysia (UTM), Malaysia. Currently, she is a lecturer at University Sultan Zainal Abidin, Terengganu, Malaysia. Her current research interest includes Information Security – Awareness and Ethics, and Security Management.

Mustafa Mamat, he is currently a Professor at Universiti Sultan Zainal Abidin (Unisza), Malaysia since 2013. He was first appointed as a lecturer at Universiti Malaysia Terengganu (UMT) in 1999. He obtained his Ph.D. from UMT in 2007 specialization in optimization field. Later on, he was appointed as a Senior Lectures in 2008 and then as an Associate Professor in 2010 also at UMT. To date, he has successfully supervised more than 30 postgraduate students and published more than 100 research papers in various international journals and conferences. His research interest includes optimization, conjugate gradient methods, steepest descent method, Broydens family and finite difference methods.

