Journal of Theoretical and Applied Information Technology
15th December 2016. Vol.94. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN IMAGE STEGANOGRAPHY ALGORITHM BASED ON LOGICAL CONNECTIVE

[1]SITI DHALILA MOHD SATAR, [1]NAZIRAH ABD HAMID, [1]FATIMAH GHAZALI, [1]ROSLINDA MUDA, [1]MOHAMAD AFENDEE MOHAMED

[1]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut Campus, 22200 Besut, Terengganu, Malaysia

E-mail: [1]{sitidhalila, nazirah, fatimah, roslindamuda, mafendee}@unisza.edu.my

ABSTRACT

In cloud computing, steganography can be employed as one of the solutions that is mainly used to protect transmitted data from any security breaches. Most of the existing steganography algorithms cannot embed a high capacity of secret message. The aim of this study is to show that the proposed algorithm can embed a high capacity of secret message without noticeable distortion to the images. The proposed algorithm is used Logical Connective to calculate a new binary number of secret message. From the experiments that have been conducted, the largest numbers of characters that can be hidden into and retrieved from the image are 32,763 characters with 55.92 PSNR value. This PSNR value can be considered as a good value, which means that the proposed algorithm can hide a high capacity of secret messages underneath the image with near-zero distortion. Hence this new steganography algorithm is very efficient to hide secret messages inside an image.

Keywords: *Image Steganography, Least Significant Bit (LSB), Logical Connective Algorithm, Cloud Computing, Information Security*

1. INTRODUCTION

The interesting features in cloud computing have been powering the integration of cloud environments with many industries, for instance, the financial and education businesses. The appealing characteristics such as the efficiency, flexibility, scalability, and pay-per-use is changing the enterprise conventional computing model to modern infrastructures that can be accessed over the Internet and managed by cloud server provider (CSP). But alongside the aforementioned advantages, the transition of these computing paradigms elevates many security concerns and one of the critical problems in the cloud environment is the issue of access control and security [1]. In this context, there are many solutions existed for each security concerns from encryption methods to access control models.

In cloud computing, steganography can be employed as one of the solutions that is mainly used to protect transmitted data from any security breaches. The key principle of steganography is to embed a secret message into a digital host such as a digital audio file, image, or video [2]. This involves two major processes. The first process is the embedding process where a secret message is embedded in the host [3] and the second process is the extracting of the secret message. Currently, image steganography has fascinated many researchers to study extensively on them compared to other types of steganography. Among the advantages of images are the capability of an image to hide large amount of data unnoticed due to the incapability of human eyes to notice any differences in the image [4].

Many steganography algorithms have been introduced to hide data especially in digital images. In general, there are three most important factors that influence the designing of a steganography algorithm. The three factors: (1) capacity, an amount of secret message that can be embedded into the host without much distortion; (2) robustness, an amount of alteration that stega-object can survive while it goes through some reprocessing operations; and (3) security, an incapability of an attacker to discover the hidden data [5]. The widely utilized hiding data technique is the Least-Significant-Bit (LSB) that manipulates the least-significant bit planes by replacing each pixel in the host image with secret message bits. The advantages of LSB include it is simple to compute and implement and has an ability to hide many data in the host without destroying the quality of the image (host) [6].

The aim of the study is to propose an algorithm that uses the logical connective in embedding and extracting processes. The proposed algorithm uses substitution technique hide text message into an image. This proposed algorithm can embed high capacity of secret message without noticeable distortion to the image. The result of the proposed algorithm shows a large amount of secret message is successfully embedded in the cover image with less distortion which is measured using the Peak Signal to Noise Ratio (PSNR).

In this study, we develop a suitable proposition of logical connective for steganography algorithm that can be used as a mechanism to hide text message into an image file. In addition, this study also describes the implementation of the proposed algorithm by developing an application and later evaluates the effectiveness of the proposed algorithm.

The remainder of this paper is organized as follows. In Section 2, related works based on LSB technique is introduced and Section 3 discussed about the methodology. In Section 4, the proposed logical connective algorithm is described. The implementation of the proposed algorithm is given in Section 5. Section 6 discussed the experimental results and Section 7 concludes this paper.

2. RELATED WORKS

The growth of digital images has directed to the development of many image steganography algorithms. Lashkari et al. [7] stated the four classifications of image steganography: (1) substitution techniques, which replace the least significant bits of the host image with the bits of secret data; (2) statistical techniques, which embed one bit of data in the host image and then generate a statistical change; (3) transform techniques, which hide the secret data in a signal; (4) spectrum techniques, which a stream of data is transmitted into small fragments.

In this section, we discuss one of the most popular substitution technique namely Least-Significant-Bit (LSB) that form the basis to the proposed method. An original image steganography technique that used the achromatic component (I-plane) of the hue-saturation-intensity (HSI) color model and multi-level encryption (MLE) was presented by [8]. This technique was easy to be implemented, able to improve the security of the secret messages and the efficiency by decreasing the required processing time. One bit-plane method was implemented by [2] and the authors applied an adaptive complexity threshold computation to choose the complex regions of a host image to hide information. This method enhanced the capability of embedding secret message and the security performance.

Akhtar, Khan and Johri [9] proposed two schemes of bit inversion technique to improve LSB steganography. This double bit inversion technique resulted in less number of pixels modified thus retained the quality of the host image. According to the authors, this technique could be combined with other techniques to enhance the development of steganography. Meanwhile a technique that introduced by [10] improved LSB method by storing the secret message bits in random order. In their technique, they used RC4 the algorithm. This technique enhanced the host image quality and it was robust against malicious attacks.

Kaur and Kaur [11] discussed a technique to hide more number of bits in a pixel. The authors proposed an algorithm that maps the secret message to one channel of the cover image and used LSB of other channel as the mark. The purpose of this marking was to indicate the presence of secret message in the channel. The authors stated that this proposed technique could provide high capacity of the secret message that can be embedded.

Meanwhile, Al-Dmour and Al-Ani [12] introduced boolean operation known as XOR in their proposed algorithm. According to the authors, the XOR operation was a simple yet effective process particularly to reduce the differences between the cover and stego-image. The proposed algorithm embedded the three bit of secret message in the selected edge of the image. However, this technique would restrict the area of the secret message that could be embedded.

In this paper, our proposed model uses Connective Logical as an algorithm to calculate a new binary number of secret. Logical connective algorithm has been developed based on propositions where it is a declarative sentence. Proposition declares the fact that is either true or false, but not both.

3. METHODOLOGY

This study involves four phases of research design as shown in Figure 1. Phase 1 started with designing the algorithm for embedding and extracting process. In this phase, every possible logical connective for both processes has been determined manually and recorded in table form. In phase 2, image steganography application was developed by using the proposed algorithm before being tested in phase 3. Lastly, in phase 4, Matlab software was used to calculate PSNR value in determine quality of the image.

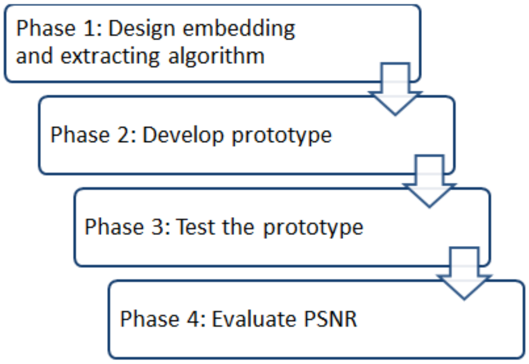
Phase 1: Design embedding and extracting algorithm
Phase 2: Develop prototype
Phase 3: Test the prototype
Phase 4: Evaluate PSNR

Figure 1: Research Design

4. PROPOSED LOGICAL CONNECTIVE ALGORITHM

The proposed logical connective algorithm is developed based on propositions where it is a declarative sentence. Propositions declare the fact that is either true or false, but not both. The area of logic that deals with propositions is called propositional logic. According to [13], the definition of propositional logic is as below:

'Let p and q be propositions. The exclusive-or of p and q, denoted by p XOR q, is the proposition that is true when exactly one of p and q is true and is false otherwise.'

Based on the above definition, the equation for logical connective algorithm is produced as below:

$$R1[i,j]= P[i,j] \text{ XOR } Q[i,j] \qquad \text{(Eq. 1)}$$

$$R2[i,j]= R1[i,j] \text{ XNOR } m \qquad \text{(Eq. 2)}$$

where;
P is most significant bit of pixel
Q is a second most significant bit of pixel
i and j are coordinates of each pixel, where i=0, 1, 2, …, n; j=0, 1, 2, …, n
m is binary digit of the secret message

The general model for the proposed logical connective algorithm for the study is as in Figure 2. In this model, the first and second bits of most significant are used to calculate the new binary number of secret message. Then, this new bit of secret message is embedded in the cover image before sending it to the receiver. This model also comprises of two main algorithms namely embedding and extraction algorithms as stated in Section 4.1 and Section 4.2.

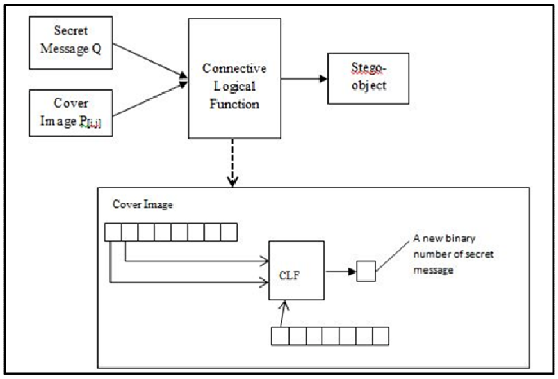
Secret Message Q
Cover Image P[i,j]
Connective Logical Function
Stego-object
Cover Image
CLF
A new binary number of secret message

Figure 2: Logical Connective Model

4.1 Embedding Algorithm

The main steps of the proposed embedding algorithm are given in Algorithm 1. In this algorithm, the XOR and XNOR operation are used to produce a new binary number of secret messages.

Algorithm 1: Embedding Algorithm

Input: An image to use as a host, a secret message

1. The image must be converted into its binary number.
2. The length of the binary number for image and secret message is compared.
3. If the length of the host more than secret message, Step 4 is performed, else end the process.
4. Select the first and second most significant bit
5. Perform exclusive XOR to both of selected pixel
6. The output then has been XNOR with the first binary number of secret

message

7. The result from Step 4 is replaced to the least significant bit of each pixel image.
8. Repeat the steps until all the secret bit value are replaced.
9. End the process

Output: A stego-image containing the secret message

4.2 Extraction Algorithm

The major steps of extraction algorithm are given in Algorithm 2:

Algorithm 2: Extraction Algorithm

Input: An image that contain the secret message

1. The image must be converted into its binary number.
2. Select the first and second most significant bit
3. Perform exclusive XOR to both of selected pixel
4. The output then has been XNOR with the least significant bit of the pixel
5. Repeat the steps until end of the secret message
6. End the process

Output: A secret message

5. IMPLEMENTATION OF THE PROPOSED ALGORITHM

In this section, the authors would demonstrate the embedding and extracting implementations of the proposed algorithm.

5.1 Embedding Process

The character of ‘U’ is selected as a secret message and chooses an image as a host image.

1. Choose a host image
2. Convert the host image to binary number
3. Insert a secret message. Let say the secret message is ‘U’
4. Convert the secret message to binary number. The binary number for letter ‘U’ is 01010101
5. Perform calculation using Eq. 1 and Eq.2 on binary digit of the secret message, Mi. Table 1 shows the results for each equation.
6. Then substitute R2i into least significant bit of each pixel.

Table 1: Experimental Result of Embedding Process.

M	Mi	Pixel[i,j]	P	Q	R1= P XOR Q	R2= R1 XNOR Mi
U	0	0,0	0	0	0	1
	1	1,0	0	0	0	0
	0	2,0	0	1	1	0
	1	3,0	0	1	1	1
	0	4,0	1	0	1	0
	1	5,0	1	0	1	1
	0	6,0	1	1	0	1
	1	0,1	1	1	0	0

After the processing is done, the stego-image will be send to the receiver. In order to get back the secret message, the receiver needs to use the application.

5.2 Extracting Process

The image received from the sender must be converted into binary number in order to acquire back the secret message.

1. The stego-image must be converted into its binary number;
2. Select the first and second most significant bit;
3. Perform exclusive OR to both selected pixel; P and Q;
4. The output then has been XNOR with the least significant bit of the pixel; The calculation for Step 3 and 4 as in Table 2;
5. Repeat the steps until end of secret message;
6. End the process.

Table 2: Experimental Result of Extracting Process.

Pixel[i,j]	LSB, Si	P	Q	R1= P XOR Q	R2= R1 XNOR LSB
0,0	1	0	0	0	0
1,0	0	0	0	0	1
2,0	0	0	1	1	0
3,0	1	0	1	1	1
4,0	0	1	0	1	0
5,0	1	1	0	1	1
6,0	1	1	1	0	0
0,1	0	1	1	0	1

The extraction process can be seen as the reverse of the embedding process. The output of embedding process is expected to be the same as the input to the embedding process. In this proposed method, we can prove the recoverabilities of the original message by simply constructing the truth table for R1 XNOR LSB = R1 XNOR (R1 XNOR Mi) which can be shown to be identical to M*i*.

6. EXPERIMENTAL RESULT AND DISCUSSION

To implement the proposed algorithm, an application is developed in Java Programming Language. This application has two main modules, sender and receiver modules. Figure 3 and Figure 4 show the application interface for the sender and receiver module while Figure 5 shows the image that has been selected as the cover image in this experiment.

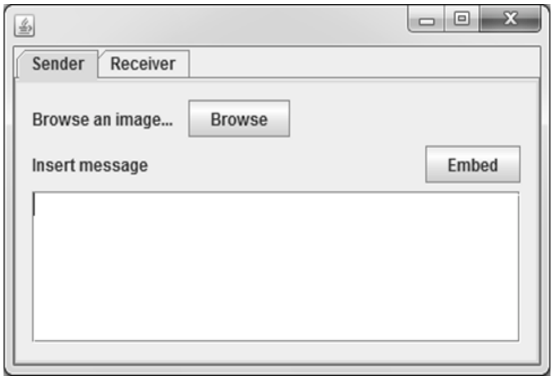

Figure 3: Sender Interface

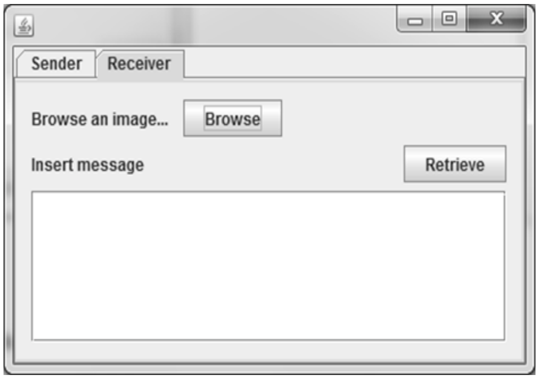

Figure 4: Receiver Interface

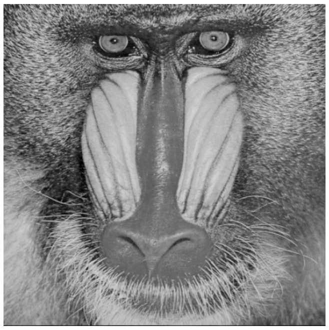

Figure 5: Cover Image

Primarily, the aim of this study is to show that the proposed algorithm can embed a high capacity of secret message without noticeable distortion to the images. The image file format used in the proposed algorithm is Portable Network Graphics (PNG) format. The application is tested using the image as shown in Figure 5. The size of the image is 512 x 512. In this experiment, the authors tested the algorithm by using the Peak signal-to-noise ratio (PSNR) to determine the quality of the stego-image. According to [14], to get a quality stego-image, the value of PSNR should be high.

Table 3 shows a number of characters of the secret message that could be embedded into the stego-image by using the proposed algorithm and the corresponding PSNR values. From the experiments that have been conducted, the value of PSNR for each round is quite similar to each other. The highest number of characters that can be hidden into and retrieved from the image are 32,763 characters with 55.92 PSNR value. This PSNR value can be considered as a good value, which means that the proposed algorithm can hide a high capacity of secret messages underneath the image with near-zero distortion.

Table 3: PSNR values.

No of Experiment	Number of characters	PSNR
1	999	71.07
2	3,999	65.03
3	7,999	62.02
4	15,999	59.04
5	31,999	56.03
6	32,763	55.92

Table 4 present the comparison of PSNR value between the proposed algorithm and [11]. The image size used in the both experiment is 512*512 in the RGB format. It is observed that, the proposed method obtain higher PSNR value compared to [11] since the proposed method manipulate least significant bit of every pixel to hide the secret message. [11] claimed that their technique can hide 7 bit per pixel, but our proposed algorithm can hide higher secret message with 7999 characters while [11] only can hide 100 characters for the same range PSNR value. Experimental result demonstrated that the proposed algorithm has achieved better imperceptibility result with high embedded capacity than other technique.

Table 4: PSNR values.

No of Experiment	Number of characters	PSNR Value	
		[11]	Proposed
1	25	64.7	86.75
2	50	63.023	83.70
3	100	60.037	81.01

In order to have a comparison between the proposed algorithm and [11], a graphical representation of the PSNR values is shown in Figure 6. It is clear that the PSNR for the proposed algorithm achieves a higher visual quality compared to [11].

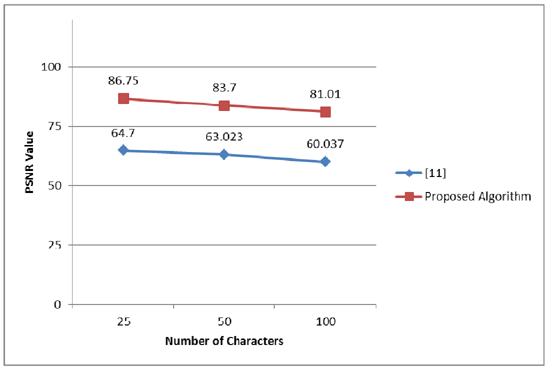

Figure 6: Comparison of PSNR

7. CONCLUSION

Primarily, the aim of this study is to show that the proposed algorithm can embed a high capacity of secret message without noticeable distortion to the image. In this paper, connective logical is used as an algorithm to calculate the new binary number of secret message. From the experiments that have been conducted, the value of PSNR for each round is quite similar to each other. The highest characters that can be hidden into and retrieved from the image are 32,763 characters with 55.92 PSNR value. This PSNR value can be considered as a good value, which means that the proposed algorithm can hide a high capacity of secret messages underneath the image with near-zero distortion.

REFERENCES:

[1] Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., and Inacio, P. R. M., “Security Issues in Cloud Environments: A Survey”, *International Journal of Information Security*, 13(2), 2014, pp.113–170.

[2] Nguyen, T. D., Arch-int, S., and Arch-int, N., “An Adaptive Multi Bit-Plane Image Steganography Using Block Data-Hiding”, *Multimedia Tools and Applications*, 2015, pp. 1-27.

[3] Satar, S. D. M., Hamid, N. A., Ghazali, F., Muda, R., and Mamat, M., “A New Model for Hiding Text in an Image Using Logical Connective”, *International Journal of Multimedia and Ubiquitous Engineering*, 10(6), 2015, pp. 195-202.

[4] Maiti, C., Baksi, D., Zamider, I., Gorai, P., and Kisku, D. R., “Data Hiding in Images Using Some Efficient Steganography Techniques”, *Signal Processing, Image Processing and Pattern Recognition,* 2011, pp. 195-203.

[5] Subhedar, M. S., and Mankar, V. H., “Current Status and Key Issues in Image Steganography: A Survey”, Computer *Science Review*, 13, 2014, pp. 95-113.

[6] Shen, S., Huang, L., and Tian, Q., “A Novel Data Hiding for Color Images Based on Pixel Value Difference and Modulus Function”, *Multimedia Tools and Applications*, 74(3), 2015, pp. 707-728.

[7] Lashkari, A. H., Manaf, A. A., Masrom, M., and Daud, S. M., “A Survey on Image Steganography Algorithms and Evaluation”, *Digital Information Processing and Communications*, 2011, pp. 406-418.

[8] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., and Baik, S. W., “A Novel Magic LSB Substitution Method (M-LSB-SM) Using Multi-Level Encryption and Achromatic Component of An Image”, *Multimedia Tools and Applications*, 2015, pp. 1-27.

[9] Akhtar, N., Khan, S., and Johri, P., “An Improved Inverted LSB Image Steganography”, *Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 2014, pp. 749-755

[10] Akhtar, N., Johri, P., and Khan, S., “Enhancing The Security and Quality Of LSB Based Image Steganography”, *Computational Intelligence and Communication Networks (CICN)*, 2013, pp. 385-390.

[11] Kaur, S., & Kaur, S. (2011). An Image Steganography Approach Based upon Matching. In High Performance Architecture and Grid Computing (pp. 603-608). Springer Berlin Heidelberg.

[12] Al-Dmour, H., & Al-Ani, A. (2016). A steganography embedding method based on

edge identification and XOR coding. Expert systems with Applications, 46, 293-306.

[13] Rosen, K. H., “Discrete Mathematics and Its Applications”, 7, 2011, New York: McGraw-Hill.

[14] Ibrahim, R. and Kuan, T.S., “Steganography Algorithm To Hide Secret Message Inside an Image”, 2011.