International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:10, 2011

A Robust Data Hiding Technique based on LSB Matching

Emad T. Khalaf and Norrozila Sulaiman

***Abstract*—**Many researchers are working on information hiding techniques using different ideas and areas to hide their secrete data. This paper introduces a robust technique of hiding secret data in image based on LSB insertion and RSA encryption technique. The key of the proposed technique is to encrypt the secret data. Then the encrypted data will be converted into a bit stream and divided it into number of segments. However, the cover image will also be divided into the same number of segments. Each segment of data will be compared with each segment of image to find the best match segment, in order to create a new random sequence of segments to be inserted then in a cover image. Experimental results show that the proposed technique has a high security level and produced better stego-image quality.

***Keywords*—**steganography; LSB Matching; RSA Encryption; data segments

I. Introduction

SINCE many years ago, the issue of important information hiding preoccupied the minds of many people especially in business, military and political fields due to the secrecy of their information. Thus, there were always secret means and methods that were pursued to send such information. After the spread of internet, information can be sent easily and quickly. However, at the same time the sent data were easily intercepted and uncovered by hackers. Researchers and scientists have made a lot of research work to solve this problem and to find an effective method for image hiding [1]. Among the methods invented was hiding information in a text or an image or an audio without changing the size of the sent file or its distortion, then sending it via internet in a way that no one can detect. This is still considered a new science in our modern age that every now and then new researches and theories emerge. One of information hiding techniques is steganography , it is the art of hiding and transmitting data apparently through innocuous carriers in order to conceal the existence of the secret data [2]. The main goal of steganography is to communicate message securely in a complete undetectable manner [3],[4]. How to keep the information transmission secured is become an important issue nowadays, including how to design an efficient technique for image hiding which is a popular topic in recent years [5],[6].

Emad T. Khalaf, Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Kuantan, 26300, Malaysia (phone: +6095492133 , fax: +6095492144, e-mail: mcc10001@stdmail.ump.edu.my)
Norrozila Sulaiman, Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Kuantan, 26300, Malaysia (phone: +6095492133 , fax: +6095492144,e-mail norrozila@ump.edu.my)

Least Significant Bit (LSB) algorithm has a larger amount of capacity than other embedding techniques and it is recognized now, due to many advantages such as the algorithm is simple, the embedded velocity is fast and so on. Compared with the hidden algorithm based on transform domain, the advantage of LSB algorithm is unparalleled. So LSB algorithm still occupies an important position in information hiding. The common steganography software in internet uses LSB algorithm or LSB derivative algorithm [7]. For encrypting the secret data, Rijndael Encryption Algorithm will be used. This algorithm which was designed by Joan Daemen (Proton World International Inc.) and Vincent Rijmen (Katholieke Univeriteit Leuven) of Belgium, is a block cipher with a simple and elegant structure [8]. The Rijndael algorithm [9] is a fast and efficient method for data encryption. In this paper, a new steganography scheme was proposed. The scheme combines cryptography and steganography, the purpose of combining cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from malicious people, whereas steganography even conceals the existence of the message[10]. The secret data will be encrypted by Rijndael algorithm first, and then the segments of the processed secret data are embedded in the cover image to fulfill steganography. Experimental results show that the proposed scheme has a high security level and better image stego-image quality. The rest of the paper is organized as follows. In Section 2 and 3 image steganography scheme was described in detail. Section 4 and 5 discuss performance measure and experimental results. Finally, the last section is the conclusion, which is presented in Section 6.
Procedure for Paper Submission

II. Steganography Techniques

Steganography is the art of embedding information in such a way that prevents the detection of hidden messages. It means hiding secret messages in graphics, pictures, movie, or sound. Steganography comes from the Greek word steganos, which means ‘covered’, and -graphy, which means ‘writing’. Covered writing has been manifested way back during the ancient Greek times around 440 B.C. Some of old steganography examples are shaving the heads of slaves and tattoo messages on them. Once the hair had grown back, the message was effectively hidden until the receiver shaved the heads once again. Another technique was to conceal messages within a wax tablet, by removing the wax and placing the message on the wood underneath [11].The most popular and frequently method of Steganography is the Least Significant Bit embedding (LSB). The level of precision in many image formats is far greater than that perceivable by average human

vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. If we are using the least significant bits of the pixels' color data to store the hidden message, the image itself is seemed unaltered [12],[13] and changing the LSB's value will have no effect on the pixel's appearance to human eye.

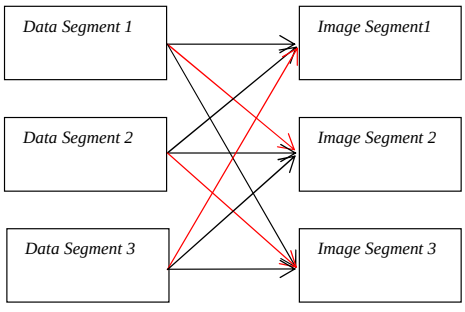
III. THE PROPOSED TECHNIQUE

In these technique, types of images can be used are BMP, PNG and TIFF images and least significant bit (LSB) insertion are used. A user is allowed to use a color or gray scale image as a cover image. Two files are requiring embedding a message into an image. The first is the message (the data to be hidden), a message may be plain-text, cipher-text, other images, or anything that can be embedded in a bit stream. The second file is the innocent-looking image that will hold the hidden information, called the cover image. The concept of the proposed image hiding technique is illustrated in Fig.1, the processes are:

Input: Cover image and secret data
Output: Stego-image

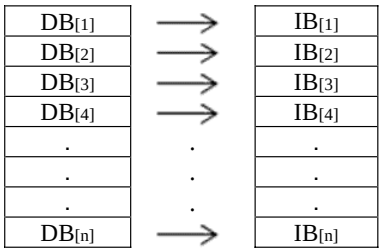
1. Encrypt the secret data by using Rijndael Encryption Algorithm after entering a secret key.
2. Convert the encrypted data and the least significant bits of cover image into bit stream. Then, divide each data and image bit streams into number of segments based on specific number entered by a user. Sizes of segments will vary, depend on the length of data and cover image. Each segment will be a matrix of bits (0,1).
3. Compare each segment of data bit by bit with each segment of cover image to find the best segment match.

For instance, User enters 'three' as a number of segments, each of the 'three' data segments will be compare with all the 'three' image segments to find the best match in order to hide it inside, the comparing process will be as follows:



From this example, the new sequence of data segments will be {2,3,1}. Comparing process involves comparing bit by bit for each segment which is shown as follows:

From this example, the new sequence of data segments will be {2,3,1}. Comparing process involves comparing bit by bit for each segment which is shown as follows:



1. After the process of comparing has completed, new random sequence will be produced for data segments to hiding them inside cover image.
2. The hiding process will start by inserting the total length of the secret data and the new segments sequence in the first 32 pixels of the beginning of the cover image.
3. Data segments will be hidden one by one based on the random sequence. Each segment bits will be hidden in the least significant bits of the cover image.
4. Finally, the cover image bit stream that contained the random data into stego-image will be converted.

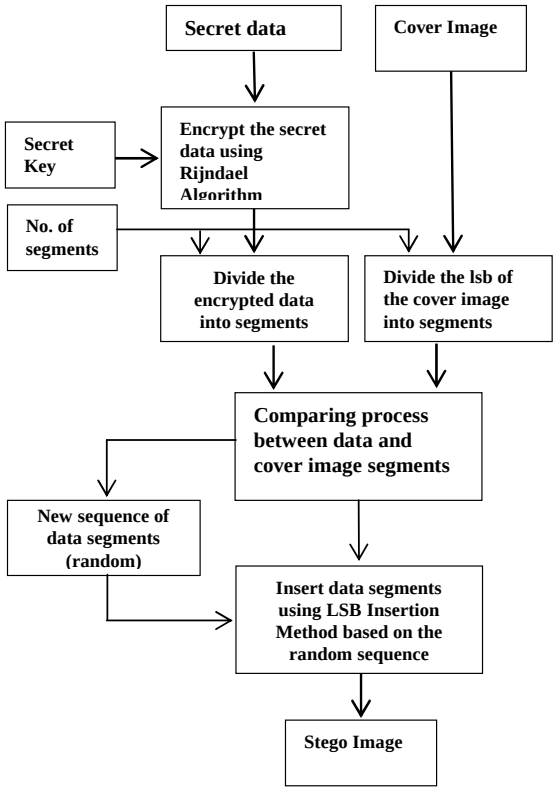


Fig. 1 Insertion processes for the proposed method

The extraction process does not need the original image, because it is a blind extraction process**.** The process of extraction method is illustrated in Fig 2, which involves the following processes:

Input: Stego-image
Output: Secret message

1. User enters number of segments.
2. The length of the data and the random sequence of data segments will be extracted.
3. After the length of each segment has been calculated, segments will be extracted one by one using the random sequence.
4. The segments will be rearranged into the original sequence.
5. Last process is decrypting the extracting data based on the entered key by a user, to get the secret data.

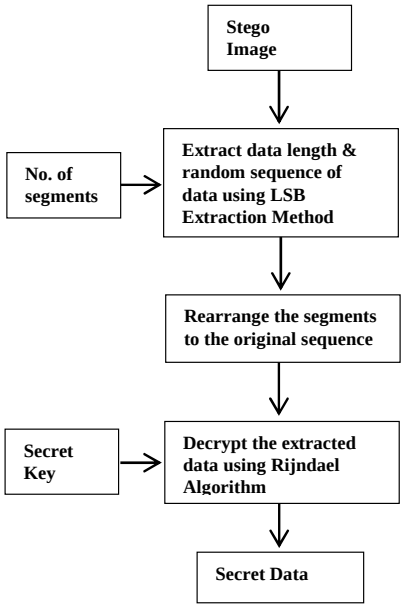


Fig . 2 Extract processes for the proposed method

IV. Performance Measure

Peak-Signal-to-Noise Ratio (PSNR) is a performance measurement for image distortion. PSNR is introduced to evaluate the performance of the proposed scheme and the image quality, which is defined as:

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})dB$$

$$MSE = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\frac{(a_{i,j} - b_{i,j})^2}{n \times m}$$

Where m ×n is the image size whereas, ai,j and bi,j are the corresponding pixel values of two images[14]. The PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30dB indicates a fairly low quality (i.e., distortion caused by embedding can be obvious). A high quality Stego should strive for 40dB and above Normalized Cross-Correlation(NCC) to evaluate this similarity with different number of segments[15].Cross correlation is a standard method of estimating the degree to which two series are correlated. Consider two series x(i) and y(i) where i=0,1,2,. . . ,N-1. The cross correlation r with delay d is defined as:

$$r = \frac{\sum_i [(x(i) - mx)(y(i-d) - my)]}{\sqrt{\sum_i (x(i) - mx)^2}\sqrt{\sum_i (y(i-d) - my)^2}}$$

where mx and my are the means of the corresponding series. The cross-correlation is used for template matching which is motivated through the following formula

$$R = \sum_x \sum_y f(x,y)T(x-u, y-v)$$

Where, f is the image and the sum is over x, y under the window containing the feature t positioned at u, v. Similarity measure of two images can be done with the help of normalized cross correlation generated from the above concept using the following formula:

$$r = \frac{\sum(C(i,j) - m1)(S(i,j) - m2)}{\sqrt{(\sum_{(c(i,j)-m1)})^2}\sqrt{(\sum_{(s(i,j)-m2)})^2}}$$

where c is the cover image, s is the stego image, $m1$ is the mean pixel value of the cover image and $m2$ is the mean pixel value of stego image. It has been seen that the correlation coefficient computed here for all the images is almost one, which indicates both the cover image and stego image are highly correlated.

V. Experiment Result

Several images have been used with different size, type and lengths of specific secret data. The experiments revealed the efficacy of the proposed technique in producing visually pleasing stego-images. The proposed scheme was tested on both color and gray-scale images, including vegetables, children, Baboon and flowers. The original images are shown in Figure 3(a, b, c, d). The stego images are shown in Figure 4(a, b, c, d) .Figure 5 shows the values of PSNR with different number of segments and for comparing the similarity between cover image and the stego image.

a b

c d

Fig. 3 cover images

a b

c d

Fig. 4 stego- images

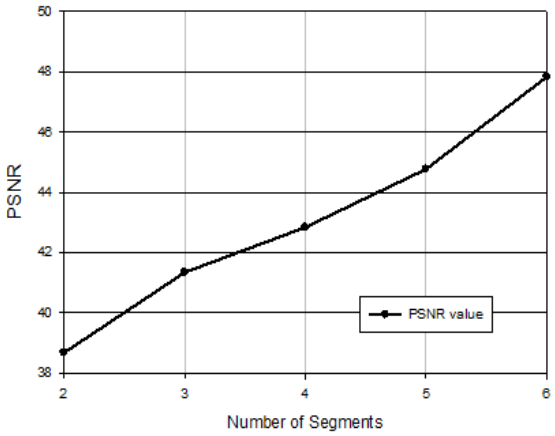


Fig. 5 The values of PSNR with different number of segments

Table I show the values of Normalized cross correlation (NCC) , the values are very close to 1 especially when the No. of segments are increasing.

TABLE I
VALUES OF NCC

Images	No. of Segments	NCC
1. Vegetables.bmp	2	0.7995
2. Children.tiff	3	0.8997
3. Baboon.png	4	0.9975
4. Flowers. bmp	5	0.9989
5. lena.png	6	1.0000

As we can see from the figures and table, the result become better if we increased numbers of data and image segments, but at the same time it affects to the speed performance of the software. This is because there are many comparisons need to be carried out when involve large numbers of segments**.**

VI. CONCLUSION

A robust steganographic technique which included two levels of security cryptography and steganography was presented. The encrypted data will be divided into specific number of segments and sequence will be changed into a random. This suggests that an image containing encrypted data which are hidden randomly can be transmitted anywhere across the world, in a complete secured form**.** This method can be used in any other application such as image watermarking, since it has a high security level and better image stego-image quality. For future improvement, its functionality will be improved to support hiding data in lossy compression images.

REFERENCES

[1] Zahra Toony and Mansour Jamzad "A Novel Image Hiding Scheme Using Content Aware Seam Carving Method" International Conference on Availability, Reliability and Security , 2010
[2] Peticolas FAP, Anderson RJ, and Kuhn MG, “Information hiding-A survey,” Proc. of the IEEE, Vol. 87, No. 7, pp.1062-1078,1999.
[3] Niels Provos and Peter Honeyman, “Hide and Seek: An Introduction to Steganography”, IEEE 1540-7993, June 2003
[4] M.M Amin, M. Salleh, S. Ibrahim, M.R. Katmin, and M.Z. I. Shamsuddin “ Information hiding using Steganography” IEEE 0-7803-7773-March 7, 2003.
[5] P. Tsai, etal. “Reversible image hiding scheme using predictive coding and histogram shifting”, Signal Processing, vol. 89. pp. 1129-1143, 2009.
[6] Emad T. Khalaf, Norrozila Sulaiman "Segmenting and Hiding Data Randomly Based on Index Channel" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011 ISSN (Online): 1694-0814
[7] Neil F. Johnson. Steganography tools. Available from: http://www.jjtc.com /Security /stegtools.htm 2005.
[8] J. Daemen and V. Rijmen, AES Proposal: Rijndael,version 2, 1999. Available from URL: http://www.esat. kuleuven.ac. be/vijmen/rijndael.
[9] Daemen J. and Rijmen V. Aes proposal: Rijndael,aes algorithm submission. Technical report, http://www.nist.gov/ CryptoToolkit, September 1999.
[10] M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin "Information Hiding using Steganography" 4* National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003.

[11] Peter Wayner,Disappearing Cryptography –Information Hiding: Steganography & Watermarking–Second Edition. San Fransisco, California, U.S.A.: Elsevier Science, 2002, ISBN 1558607692.
[12] Neil F. Johnson and Sushil Jajodia, Exploring Steganography: Seeing the unseen IEEE transaction on Computer Practices. 1998.
[13] Ross Anderson, Roger Needham, Adi Shamir, The Steganographic File System, 2nd Information Hiding Workshop, 1998.
[14] Emad T. Khalaf and Norrozila Sulaiman " A New Method of Image Watermarking Based on Lowest Effective Bits" 2011 3rd International Conference on Machine Learning and Computing (ICMLC 2011) February 26-28, 2011, Singapore ,V5-504
[15] A. Sverdlov, S. Dexter, and A. M. Eskicioglu, "RobustDCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies," Proc.European Signal Processing Conference, Turkey, 2005.

Emad T. Khalaf Graduated in Computer Information Systems and Informatics Engineering and he worked as a Technical in Internet Services Company for more than nine years. He had experience as a trainer for various computer courses. His research interests include network technology and security. He is currently studying MSc degree in the area of computer networks security.

Norrozila Sulaiman Graduated from Sheffield Hallam University with a BSc (Hons) in Computer Studies in 1994.She worked with Employment Service in UK as a network support assistant and she involved on a research on Novell Netware. After graduated, she worked as a research officer at Artificial Intelligence System and Development Laboratory and involved in joint collaboration projects between the government of Malaysia and Japan for about 5 years. She completed her MSc degree in Information Technology and involved in a research on Wireless Application Protocol (WAP). She obtained her PhD degree in mobile communication and networks from Newcastle University in UK. Currently, she is a senior lecturer at Faculty of Computer System and Software Engineering, University Malaysia Pahang. Her main research interests include heterogeneous networks, mobile communication networks and information security.