AWERProcedia
Information Technology
& Computer Science

Vol 04(2013) 447-453

3rd World Conference on Innovation and Computer Sciences 2013

Anti-Forensic Steganography Method Based On Randomization

Emad T. Khalaf *, Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Kuantan 26300, Pahang, Malaysia.

Norrozila Sulaiman, Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Kuantan 26300, Pahang, Malaysia.

Muamer N. Mohammad, State Company for Internet Services, Ministry of Communications, Baghdad 10001, Iraq.

Suggested Citation:

Khalaf T., E., Sulaiman N. & Mohammad N., M. Anti-Forensic Steganography Method Based On Randomization.*AWERProcedia Information Technology & Computer Science*. [Online]. 2013, 04, pp 447-453. Available from: www.awer-center.org/pitcs

Received November 03, 2012; revised January 25, 2013; accepted March 09, 2013.
Selection and peer review under responsibility of Prof. Dr. Fahrettin Sadıkoglu, Near East University.

Abstract

Information hiding is a technique that embeds secret information into digital contents such as images, audios, movies, documents, etc. This work presents an anti-forensic steganography method that can embed and extract messages from images, which uses the same principle of LSB. The proposed model combines cryptography and steganography. First, the secret information are encrypted using Rijndael Encryption Algorithm. Then, the cover image is divided into several matrices. The number of matrices will be determining by a user, by entering a number, which will also be used to generate a set of random numbers. However, these random numbers will be the index to hiding the encrypted data bits randomly in the least significant bits of pixel channels. This randomization is expected to increase the security of the system as well as the capacity. The metric used for image quality are Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (Corr). Experimental results show that the proposed method can provide high data security and capacity.

Keywords: Steganography, Information hiding, LSB insertion, randomization;

*ADDRESS FOR CORRESPONDANCE: **Emad T. Khalaf**, Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Kuantan 26300, Pahang, Malaysia, *E-mail Address:* emadkhalaf@gmail.com

1. Introduction

In general, connection to Internet does not use secure links, thus information that is being transferred may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is an issue nowadays and ways to give an effective method for image hiding is an interesting topic in recent years [1],[2].

Image hiding technique is an important method to realize image encryption. A technique called steganography is a technique of hiding information in digital media. In contrast to cryptography, it does not to keep others from realizing the hidden information but it is to keep others from thinking that the information even exists [17]. The main goal of steganography is to communicate message securely in a complete undetectable manner [3],[4]. Since hundred years ago, human beings had used secret writing and steganography to hide and protect information [5]. Covered writing has been manifested way back during the ancient Greek times around 440 B.C. Herodotus wrote in his text, Histories, that Histories shaved the head of his slave and tattooed it with a message. After the hair grew back, the message would be undetected until the head was shaved again [6], and with the advent of digital technology, hiding data began to take a new form by hiding data within an unsuspicious cover media is among these digital techniques. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are including [7]: (i) Least significant bit insertion (LSB), (ii) Masking and filtering, (iii) Transform techniques. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography [8]. LSB algorithm has a large amount and it is recognized now. At the same time, it have many advantages such as the algorithm is simple; the embedded velocity is fast, etc. [16]. 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. Almost all of the steganography algorithms find the trace of LSB algorithm. The common steganography software in Internet uses LSB algorithm or LSB derivative algorithm [9]. About encrypting the secret data and the seed Rijndael Encryption Algorithm are used, this algorithm designed by Joan Daemen (Proton World International Inc.) and Vincent Rijmen (Katholieke Univeriteit Leuven) of Belgium. It is a block cipher with a simple and elegant structure [10]. The Rijndael algorithm [11] is a fast and efficient method for data encryption. In the following sections, first a brief description of concepts and available methods are presented followed by a detailed description of proposed techniques and their implementation results.

Nomenclature

LSB	Least significant bit
PSNR	Peak Signal to Noise Ratio
Corr	Correlation Coefficient
MSE	Mean Squared Error

2. The proposed Method

Most steganographic methods also encrypt the message so even if the presence of the message is detected, deciphering the message will still be required. Steganography is complementary to cryptography because it adds an extra layer of security. Therefore both steganography and

cryptography were used in this study. The process of insertion method is as shown in Figure 1. The processes are:

1. Encrypt the secret data by using Rijndael Encryption Algorithm after entering a secret key.
2. Enter the value of one of the matrix dimensions to calculate the number of matrix elements (The entered value must be equal or greater than 3). A digital image is a two dimensional matrix where its elements consist of numbers that represent light intensities value at various points, and the elements are called pixels. These pixels make up the images raster data. In the case of color images, and usual color system is the RGB. In the case of full color displays, 8 bits are used for each color channel. Therefore, there are 24 bits for color representation. To calculate numbers of matrix elements the following are used:

E= D X D
Where D is the value of one of the matrices dimensions (D ≥ 3) and E is the number of matrix elements

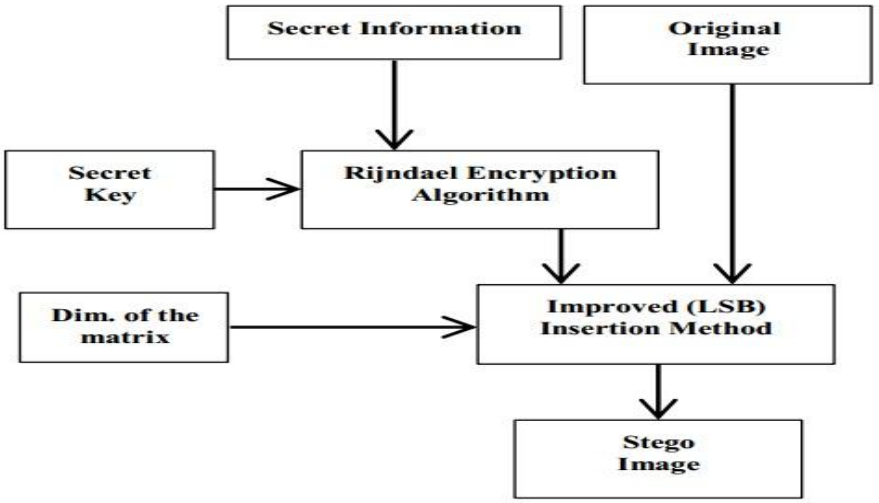
3. Use the value E to generate the random sequence by using the MATLAB function RANDPERM (E), this function returns a random permutation of the integers from 1 to input value passed to it [12].
4. Distribute each bit of encoded information inside the two-dimension matrix randomly depending on the random sequence that generate from the MATLAB function RANDPERM. In the proposed method, the improved LSB technique is used to insert encrypted data. For example, suppose there are 8 bits of encrypted data (11010010) and this matrix that contained the cover image:

The value of one of the matrix dimensions (D) = 4, the number of matrix elements (E) = 16 Then, the random sequence generated from RANDPERM function is [6 3 16 11 7 14 8 5 15 1 2 4 13 9 10 12]:

01111110	11010011	00010100	10110111
01110110	00101000	10111001	01000100
11111001	10101011	11111111	11101010
10101010	01010010	10101110	11100011

After inserting the data (11010010), the image will then become:

01111110	11010011	00010100	10110111
01110110	00101000	10111001	01000100
11111001	10101011	11111110	11101010
10101010	01010011	10101110	11100010



The process of extraction method is as shown in Figure 2. Started, by:

1. User enters the value of one of the matrices dimensions to calculate the number of matrix elements.
2. Then this number will be used by RANDPERM function to generate the random sequence.
3. Recompile the required bits after extract them to get the encoding data.
4. Finally, enter the secret key and decrypt the encoding data to get the secret information.

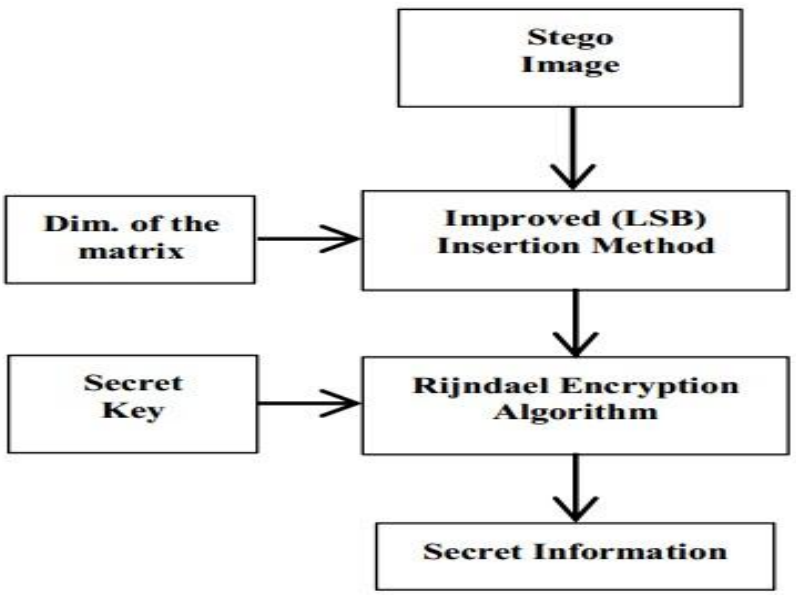


Figure 2. Extract processes

3. Image Quality Measures (IQMS)

In order to quantitatively evaluate the success of the proposed method, some of the well-known IQMs are employed: Mean Squared Error (MSE), Correlation Coefficient (Corr) and Peak Signal to Noise Ratio (PSNR). The quality measure of PSNR is defined with:

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})dB \tag{1}$$

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

Where m ×n is the image size, ai,j, and bi,j, are the corresponding pixel values of two images[13],[14],[15]. Pearson Correlation Coefficient (Corr) is given by,

$$Corr = \frac{\sum\sum(S - \bar{S})\ (Y - \bar{Y})}{\sqrt{\sum\sum(S - \bar{S})^2 \sum\sum(Y - \bar{Y})^2}} \tag{3}$$

Where

$$\bar{S}\ \frac{\sum\sum S}{M\ N} \quad and \quad \bar{Y} = \frac{\sum\sum Y}{M\ N} \tag{4}$$

S represents the pixels of the original image and Y represents the pixels of the stego- image.

4. Experiment results

Simulations are conducted on the images shown in the Figure 3(a,b,c,d) they have been used as Cover Images. The message information is embedded only in the last bit (LSB) of the cover image. In the other realizations, the message information is embedded in the last bit of the cover image randomly. As can be seen from Figure 4(a,b,c,d), embedding information into cover image causes some distortions. The effect of the distortions are evaluated with IQMs and tabulated in Table1.

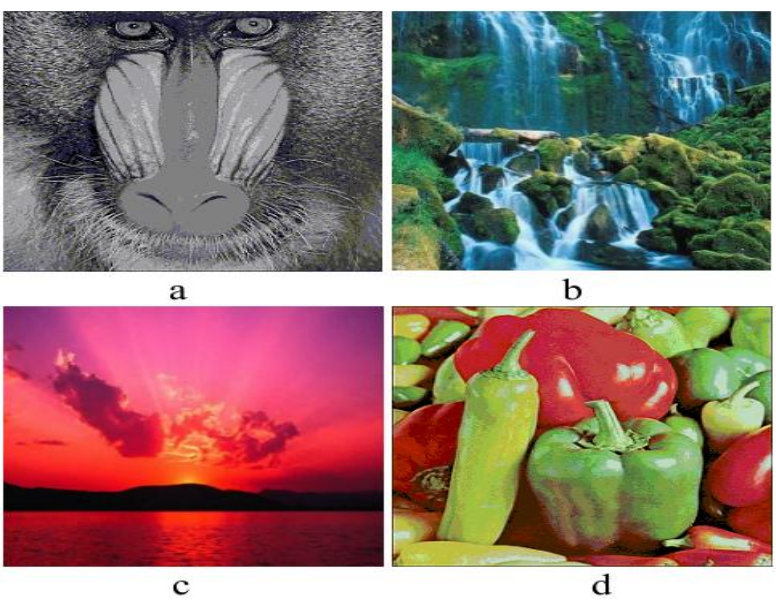


Figure3. The cover images

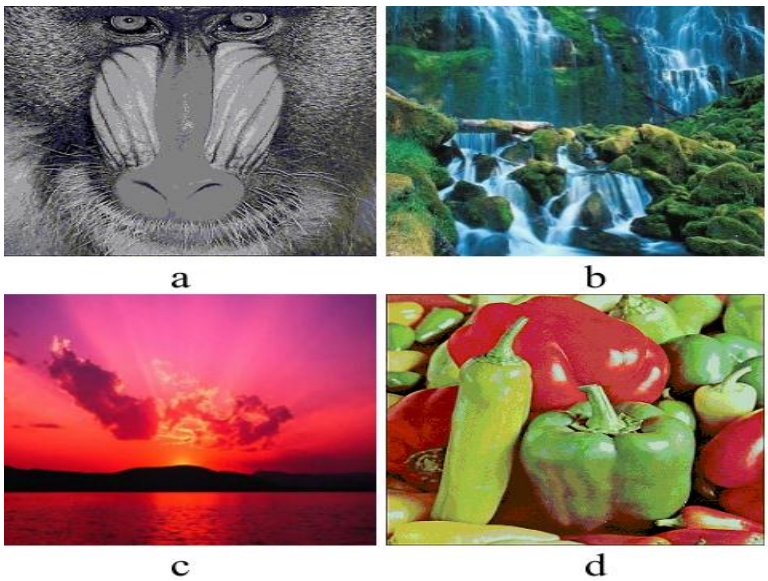


Figure4. The stego images

Table1. shows the values of PSNR and Corr

Images	PSNR	Corr
1. bmp baboon 512x512	79.6822	0.9997
2. tif waterfall 128x128	68.5802	0.9999
3. png Sunset 256x256	70.9625	0.9998
4. png lena 512x512	77.2338	0.9989
5. bmp pepper 256x256	75.9206	0.9992

5. Conclusion

In this paper, an improved scheme using the LSB matching method to hide the secret information in images was proposed and tested with various samples. To add more security, an encryption and decryption algorithm for the message before hiding were used. The most important property of this method is that the message information is scattered randomly over the last bit of the cover image pixels. The experimental results show that it does not only keep the acceptable image quality and security but also enhance convenience for transmission in the proposed scheme.

References

Tsai, P., et al., Reversible image hiding scheme using predictive coding and histogram shifting, *Signal Processing* , 2009, 89(6), pp 1129-1143.

Sajedi, H. and Jamzad, M. *Cover Selection Steganography method Based on Similarity of Image Blocks*, Int. IEEE 8th Conference on Computer and Information Technology, Tehran, 2008, pp 379 – 384.

Niels, P. and Peter, H., Hide and Seek : An Introduction to Steganography, *Security & Privacy, IEEE*, 2003, 1(3), pp 32 - 44

Amin, M., et al., *Shamsuddin Information hiding using Steganography*, Telecommunication Technology, 4th National Conference, Malaysia, 2003, pp 21 – 25.

Steinder M., et al., *Progressively Authenticated Image Transmission*, Military Communications Conference, USA, 1999, pp 641-645.

Levicky, D., et al., *A novel JPEG steganography method secure against histogram steganalysis*, 54th International Symposium ELMAR, Slovakia, 2012, pp 79 – 82.

Johnson, N. and Jajodia, S., Exploring Steganography: Seeing the Unseen, *Computer,* 1998, 31(12), pp 26 – 34.

Isbell, R., *Steganography – hidden menace or hidden savior* , 49,Publication Details, Steganography, 2002, pp 1462 -1401.

Karim, S. et al., *A new approach for LSB based image steganography using secret key*, Computer and Information Technology (ICCIT), 2011 14th International Conference, Bangladesh, 2011, pp 286 – 291.

Daemen, J. and Rijmen, V., *AES Proposal: Rijndael,version 2*, Available from URL: http://www.esat.kuleuven.. ac.be/vijmen/rijndael, 2013.

Daemen J. and Rijmen V. *Aes proposal: Rijndael,aes algorithm submission*. Available from URL: http://www.nist.gov/CryptoToolkit, 1999.

mathworks, *Random permutation*, Available from URL: http://www.mathworks.com/help/techdoc/ref/randperm.html, 2013.

Lu, C. and Liao H., Multipurpose watermarking for image authentication and protection, *Image Processing, IEEE Transactions*, 2011, 10(10), pp1579-1592.

Peng, Y. et al., *Fragile watermarking self-embedded authentication algorithm of color image*, Electronic and Mechanical Engineering and Information Technology (EMEIT), China, 2011. pp 2773 – 2776.

Eng, H. and Ma, K., Noise Adaptive Soft-Switching Median Filter, *Image Processing*, 2001, 10(2), pp 242-251.

Mishra, B. and Dhabariya, A. S., An Improved LSB Information Hiding Algorithm and Its implementation by using 'C' Language, *International Journal of Engineering Research & Technology (IJERT)*, 2012,1(10), pp 2278-0181.

Dixit P. and Bombale, U., Arm Implementation of LSB Algorithm of Steganography, *International Journal of Engineering and Advanced Technology (IJEAT)*, 2013, 2(3), pp 575 – 578.