Journal of Engineering and Applied Sciences 12 (Special Issue 11): 9176-9181, 2017
ISSN: 1816-949X

An Efficient Methods for Hiding Secure Image in Image

Baheeja Khudair Shukur and Hussein Ali Hussein
College of Information Technology and Engineering, Babylon University, Hillah, Iraq

Abstract: In this thesis, the proposed system consists of two phases. The first phase is hiding a secret image in the cover image that consists of two steps, the first step is pre-processing of secret image is which applying (FMM, minimum value subtract, improve FMM protocol) with size 8×8 pixels to reduce file size of secret image. Then applying the confusion and RC4 encryption with the key used to increased security of the secret image. The second step is the pre-processing of cover image is which dividing the cover image to six blocks accordant to some equation, arranging blocks are not sequential in one-dimensional index array, applying primary equation which is used to determine locations of the bytes where the hiding operation will be applied on it and then embedding bits of secret message in locations of the bytes depending on the above step. The second phase is extracting the secret message from the stego image that consists of number of steps (dividing of cover image, primary equation, extract algorithm, RC4 for decryption stream of bits, inverse confusion, inverse improve FMM protocol, minimum value summation and inverse compression (FMM)). In this thesis, we reach more security through the use of the proposed system. We are used some measures for performance measurement of compression and encryption randomness like) compression factor, saving percentage, NCC and PSNR). In this thesis, we have achieved good results to make a stream of bits for secret image is more randomness and high PSNR and a little time to hide and extract the security image, the results were compared with previous studies the results were better from it.

Key words: Digital image, improve FMM protocol, RC4, confusion, hiding algorithm, randomness

INTRODUCTION

Image compression methods aim at representing an approximation of original images with as few bits as possible while controlling the quality of these representations. Nowadays, image compression techniques are very common in a wide area of researches. The two types of image compression which have been introduced are lossless and lossy compression. With lossless compression, the ability to reconstruct the original image after compression is exact. On the other hand in lossy compression the ratio can be obtained with some error between the original image and the reconstructed image. In many cases, error-free reconstruction of the original image may be impossible. If the image has some noise, then there are noising methods that can be used to reduce that noise. Therefore, lossy compression may produce an acceptable error that does not affect the original image too much. This can be seen in fast transmission of still images over the internet where the amount of error can be acceptable (Todd, 2005; Pennebaker and Mitchell, 1993).

Also data encryption is a product of the information theory area of mathematics, an area that addresses various ways to manage and manipulate information. Also cryptography contains two basic processes: one process is when recognizable data, called plain data is transformed into an unrecognizable form called cipher data to transform data in this way is called to encipher the data or encryption. The second process is when the cipher data is transformed back to the original plain data, this is called to decipher or decrypting the data. To be able to determine if a user is allowed to access information a key is often used. Once a key has been used to encipher information, only the one who knows the correct key can decipher the encrypted data. The key is the foundation of most data encryptions algorithms today. A good encryption algorithm should still secure even if the algorithm is known (Petkovic and Jonker, 2009; Kahate, 2008). In addition to that steganography means: can be seen as the complement of cryptography whose goal is to hide the content of the message as the goal of steganography is to hide the presence of a message and to create a covert channel (El-Emam and Al-Zubidy, 2013).

Improve FMM protocol: The development is made on a stream of max length-bits (Jassim and Qassim, 2012) which needs 6 bits for the stored max value that represents

Corresponding Author: Hussein Ali Hussein, College of Information Technology and Engineering, Babylon University, Hillah, Iraq

the length of the maximum which will be the standard length for all other values in that stream for each new pixel coordinate that will follow. When the max length of max value for any block cannot be more than 6 bits, the development is done by decreasing the maximum length for max value in the block, the max value 48 is represented in binary 110000, the number bits of 110000 is 6 bits, the number 6 in binary is 110 and the 3 in binary is 011. Thus, we decrease max length from 6 to 3 bits in each block. The number of bits reserved for image in traditional FMM protocol is 1024 (numbers of blocks)*13(number of bits for each block)*3(R, G, B) equals (39936) but after applying the improved FMM protocol become (1024*10*3) equal to 30720. Figure 1 shows the improved FMM protocol. In this step, the resulted secret image from minimum value subtract operation will convert to stream bits.

Confusion: We make a confusion process for the stream bits produced from the improved FMM stream protocol where the stream is divided into a stream of 8 bits. Next, each twice bits for each 8 bits compare. If they are same, the first bit remains without any change and the second bit becomes 1. Otherwise, the second bit becomes 0. The operation is repeated between the first bit with the third bit and the fifth bit with the seventh bit and so on illustrated in Fig. 2. The purposes of this process is to increase security of the secret image through the scattered bits of that image and the other, if the attacker discovered the encryption method and the key used for encryption, he found difficult to detect bits of secret image.

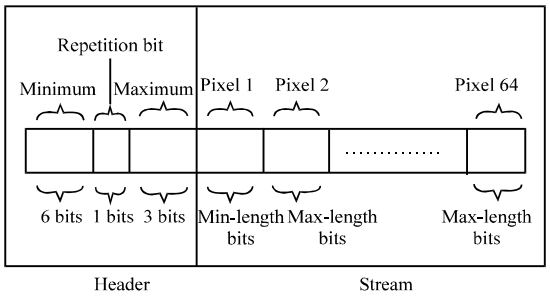

Fig. 1: Improves stream FMM protocol

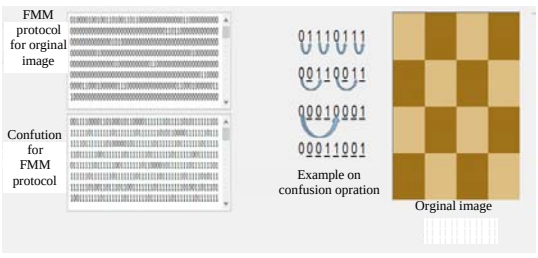

Fig. 2: Confusion for improve FMM stream protocol

MATERIALS AND METHODS

Encryption: We will decode the stream bits of secret image using traditional RC4 method. The key consists of (numbers or character) or (numbers and character). The purpose from this step is to make the stream bits of secret image more secure to avoid detection by an authorized person.

Split of cover image: In this step divide the 2D array into blocks. The numbers of the blocks are 6 blocks. The size (M*N) of each one is different from the others. Where each block size is determined according to special equations. These blocks then converted to one-dimensional array (Fig. 3).

Convert the cover image to index: Division process for the 2D array to three arrays have been made, each array represent one color. Then convert these arrays into one-dimensional array. The one-dimensional array is an index for the locations of 2D arrays of cover image. Where each location contents fourth information. The first information represents number of block for the 2D color array. The second information represent coordinate (X-axis, Y-axis) of 2D color array. The third information represent colors (R = 1, G = 2, B = 3) of 2D color array. The fourth information represents value of color for the 2D as shown in Fig. 4.

Determine bytes locations: To determine the bytes locations the primary equation have been used which derived from primary numbers to be more difficult to discover by the attackers and intruders. Equation 1 selected of the bytes locations in array one-dimensional:

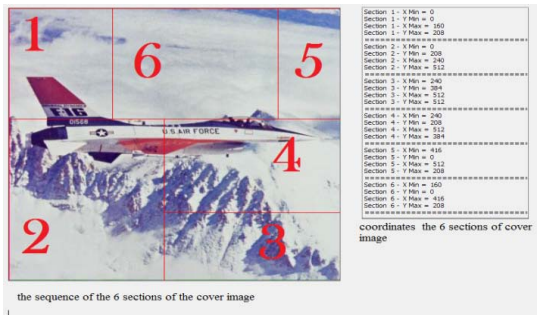

Fig. 3: The implementation of the sequence and coordinates the 6 blocks of the cover image

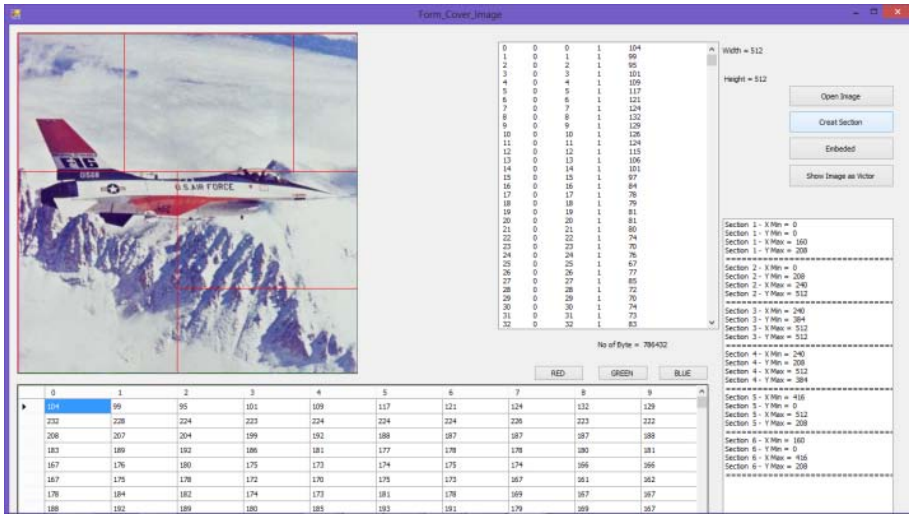

Fig. 4: The implementation of convert the cover image to array one dimension

$$d = (((i*42727) \text{ Mod no.})+17 \quad (1)$$

Where:

i = Location of array one-dimensional length
d = Location of byte
no. = Array one-dimensional length 18

The purpose of this step is to select the bytes locations in one-dimensional array for hide stream bits of secret image.

Extracting the secret message: Extracting the secret message from the stego image consists number of steps (dividing of cover image, determining the hiding byte location, extract algorithm, RC4 for decryption stream of bits, inverse confusion, inverse improve FMM protocol, minimum value summation and inverse compression (FMM).

Performance measures

Performance measures of the proposed: The performance of the proposed algorithm has been checked using two measures; these measures have been discussed through the Mean Square Error (MSE) that returns cumulative squared error between the original image and the reconstruct image, Eq. 2 and the Peak Signal to Noise Ratio (PSNR) that returns the ratio of the maximum signal to noise between two images (original, reconstruct), Eq. 3 in decibels. The best values of error measures are gotten when the MSE is low and the PSNR is large:

$$MSE = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \frac{\left(original(i,j) - Reconstruct(i,j)\right)^2}{M \times N} \quad (2)$$

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \quad (3)$$

Measures of performance compression

Compression factor: It is the inverse of the compression ratio. That is the ratio between the size of the source file and the size of the compressed file:

$$\text{Compression factor} = \frac{\text{Size before compression}}{\text{Size after compression}} \quad (4)$$

Saving percentage: Calculates the shrinkage of the source file as a percentage:

$$\text{Saving percentage} = \frac{\text{Size before compression} - \text{Size after compression}}{\text{Size before compression}}\% \quad (5)$$

RESULTS AND DISCUSSION

Results of the improve (FMM) compression: To test the improve FMM compression algorithm number of images have been used of size 256*256 pixel, these images include natural images and texture image as illustrated in Fig. 5. Figure 5 shows the image before compression and the reconstructed one after the compression.

Table 1 contains the results of measuring the performance of the improved FMM compression of different images for Fig. 5 using two measurements. The first one is the compression factor and the second is saving the percentage and content of the file size after compression.

Table 1: Performance measure of images compression

Source file Name (256*256)	Proposed system (improve FMM compression) Compressed file size (byte)	Compression factor	Saving (%)
Image 1	21849	2.999445	66.6604990
Image 2	27924	2.346924	57.3910390
Image 3	27026	2.424954	58.7621050
Image 4	33302	1.967873	49.1837183
Image 5	31379	2.088516	52.1191270

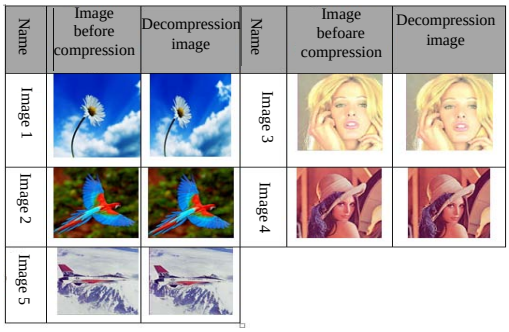

Fig. 5: Images groups of dimensions (256×256) pixels before compression and decompression

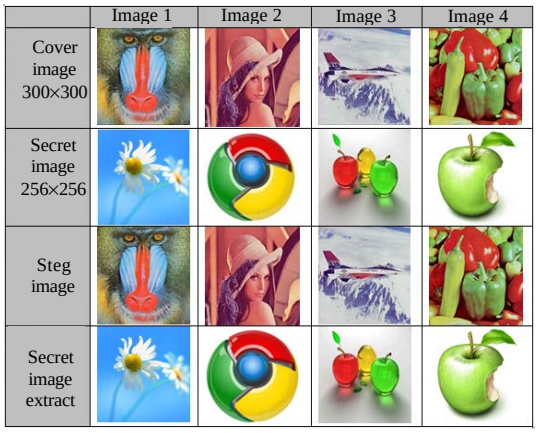

Fig. 6: Different images testing four secret images and four cover image

Result hides the secret images in cover image: There are two general cases for testing hiding images of the proposal system. The first is hiding secret image (256*256) inside cover image (254*254). The second case is hiding secret image (256*256) inside cover image (300*300).

Case 1; Hiding the secret images in cover image (300*300): In this case, we can hide secret image has size (256*256) inside cover image has size (300×300) as illustrated in Fig. 6. Since, the size of a cover image is larger than the size of the secret image.

Table 2: Performance cover image

Cover images	Channels (R,G,B)	Secret images	PSNR	NCC
1	All	1	44.51	0.9996
2	All	2	44.31	0.9993
3	All	3	44.56	0.9994
4	All	4	44.80	0.9995

Table 3: Performance secret image and hiding with extracting timing

Cover images	Channels	Secret images	PSNR images	Time for hiding (sec)	Time for extracting (sec)
1	All	1	45.61	1.572	1.552
2	All	2	46.94	1.697	1.646
3	All	3	45.24	1.490	1.468
4	All	4	47.40	1.386	1.374

Table 4: Performance cover image

Cover images	Channels (R, G, B)	Secret images	PSNR	NCC
1	All	1	44.42	0.9996
2	All	2	45.31	0.9994
3	All	3	44.74	0.9996
4	All	4	44.42	0.9987

The experimental results in Table 2 have been considered on many color images to check the performance. The results illustrate that the quality of stego image Stg has been reached according to those measures. In addition, results show that the high quality has been reached when PSNR is large and NCC tends to one. Therefore, when the stego image 4 and the secret image 4 the relative quality in the maximum while when the stego image 2 and the secret image 2, the relative quality in the minimum.

The experimental results in Table 3 have been considered on many color images to check the performance. The results illustrate that the quality of secret image has been reached according to PSNR measure. In addition, results show that the high quality has been reached when PSNR is large. Therefore, when the stego image 4 and the secret image 4 the relative quality in the maximum while when the stego image 3 and the secret image 3, the relative quality in the minimum. The minimum time of hide and extract for secret image 4. While the maximum time of hiding and extracting for secret image 2.

Case 2; Hiding the secret images in cover image (384*384): In this step can hiding secret image has size 256*256, whatever the details and intricacies of carrying inside cover image has size (384*384) as show Fig. 7.

The experimental results in Table 4 have been considered on many color images to check the performance. The results illustrate that the quality of

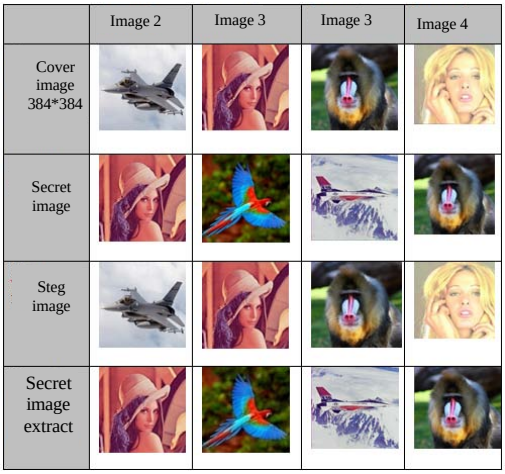

Fig. 7: Different images testing four secret images and four cover image

Table 5: Performance secret image and hiding and extracting timing

Cover images	Channels (R, G, B)	Secret image	PSNR	Time for hiding (sec)	Time for extracting(sec)
1	All	1	45.11	3.782	3.743
2	All	2	45.67	2.783	2.694
3	All	3	45.11	3.376	3.352
4	All	4	45.09	3.835	3.784

stego image Stg has been reached according to those measures. In addition, results show that the high quality has been reached when PSNR is large and NCC tends to one. Therefore, when the stego image 2 and the secret image 2 the relative quality in the maximum while when the stego image 2 and the secret image 2, the relative quality in the minimum.

The experimental results in Table 5 have been considered on many color images to check the performance. The results illustrate that the quality of secret image has been reached according to PSNR measure. In addition, results show that the high quality has been reached when PSNR is large. Therefore, when the stego image 2 and the secret image 2 the relative quality in the maximum while when the stego image 4 and the secret image 4, the relative quality in the minimum. The minimum time of hide and extract for secret image 2. While the maximum time of hiding and extracting for secret image 4.

Structural design of the suggested system: The suggested system can be seen in Fig. 8. In Table 6, a comparative study with other researchers has been taken up with the same circumstances (same cover images, same secret images and same image size) for the image in Fig. 9. These comparisons are applied between the proposed approach and the two previous according to the value of PSNR. The results confirm obviously that the proposed

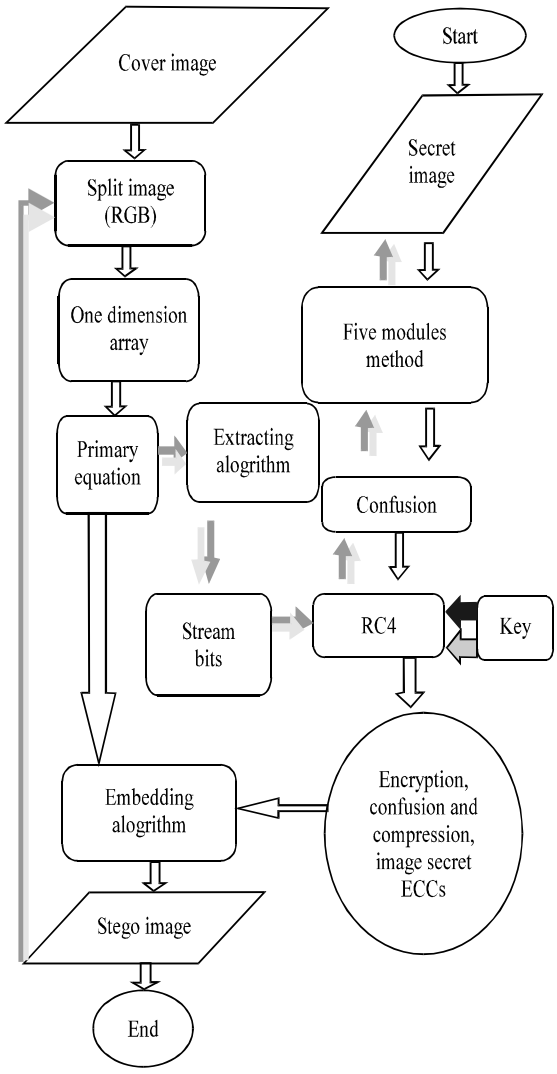

Fig. 8: Structural design of the suggested system

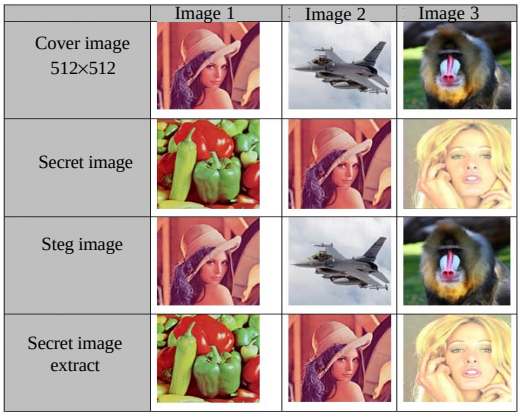

Fig. 9: Different images testing three secret images and three cover image

Table 6: Comparison performance with other researcher researches

Cover images 512×512	Channel (R, G, B)	Secret images	PSNR (Al-Shatanawi and El-Emam, 2015)	PSNR (El-Emam and Al-Zubidy, 2013)	PSNR proposal system	The percentage to improve the other researches (Al-Shatanawi and El-Emam, 2015; El-Emam and Al-Zubidy, 2013) (%)
1	All	1	39.47	42.96	47.89	10.14, 17.44
2	All	2	38.09	44.99	46.92	4.09, 18.80
3	All	3	38.12	42.47	47.60	10.07, 19.89

method is more secure and preserved secret information than the other steganography schemes. It appears that the average of three stego images in the proposed approach is better than (Al-Shatanawi and El-Emam, 2015; El-Emam and Al-Zubidy, 2013) about 18.71 and 8.1%, respectively.

CONCLUSION

The system is considered stronger and have more security against the attacker because the methodology of an algorithm that is based on randomization. The randomization comes from the following:

- Applying of FMM compression output where compression process is considered as a stream of semi-random bits
- Applying confusion in this case scatters the stream of bits according to the algorithm and makes them random
- Applying RC4 algorithm in this case encodes the stream of bits with the use of the encryption key for an increased security
- Applying dividing algorithm of cover image. For finding more random of blocks, also for more secure we used the following steps

The applying index array for bytes locations order which that non-sequential and more random. The applying primary equation for the bytes locations selection where stream bits hidden which made it random to increased security.

REFERENCES

Al-Shatanawi, O.M. and N.N. El-Emam, 2015. A new image steganography algorithm based on Mlsb method with random pixels selection. Intl. J. Network Secur. Appl., 7: 37-53.

El-Emam, N.N. and R.A.S. Al-Zubidy, 2013. New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm. J. Syst. Software, 86: 1465-1481.

Jassim, F. and H. Qassim, 2012. Five modules method for image compression. Signal Image Process. Intl. J., 3: 19-28.

Kahate, A., 2008. Cryptography and Network Security. 2nd Edn., McGraw-Hill Education, New York, USA.,.

Pennebaker, W. and J. Mitchell, 1993. Still Image Compression Standard. Van Nostrand, New York, USA.

Petkovic, M. and W.P. Jonker, 2009. Special issue on secure data management. J. Comput. Secur., 17: 1-3.

Todd, R.R., 2005. Digital Image Sequence Processing, Compression and Analysis. Taylor & Francis, Milton Park, Didcot, UK., ISBN:9780849315268, Pages: 272.