Improving the F5 Steganography Method through Shrinkage Mapping

Ali Akbar hashemi , Navid daryasafar

Abstract— There are a lot of methods for embedding hidden information in JPEG format but no method have been presented so far with a high capacity and same accuracy. The loss of JPEG compression and the effects of such compression on the images have prevented the location area from being easily used for embedding and most of the methods apply the DCT coefficients of JPEG algorithm for this aspect. This paper illustrates the shrinkage phenomenon which happens during F5 embedding process. It also shows all of the effects of shrinkage on F5 algorithm and presents a new F5 model based on the original method in order to reduce the shrinkage rate. The suggested method controlled the shrinkage rate by making a shrinkage map. Afterward, a comparison would be performed between the suggested method and the common F5me. Of course, considering the main factors of steganography such as embedding capacity and image quality, it indicates how the suggested method provides more capacity for embedding and preserves the image quality.

Index Terms— Steganography, JPEG images, F5 method, shrinkagemapping

1 INTRODUCTION

Steganography is the art of invisible communication which aims to hide the communication through embedding the massage into a cover medium in a way that it causes the least discoverable change and the existence of the hidden massage cannot be revealed even by chance [1].

The main difference between cryptography and steganography is that cryptography aims to hide the content of the massage, not its entire existence. When the exchange of the coded information causes problem, the existence of the communication should be hidden [2].

On the contrary, steganalysis is the art of discovering the existence of invisible communication and aims to distinguish between the images which contain data and the normal ones.

Ali Akbar hashemi is with Department of Communication, Bushehr Branch, Islamic Azad University Bushehr, Iran.(phone:+989171743384 ; e-mail: saa.hashemi1@yahoo.com).

Navid daryasafar is with Department of Communication, Bushehr Branch, Islamic Azad University Bushehr, Iran.(phone:+989173730829 ; e-mail: navid_daryasafar@yahoo.com).

Just like steganograohy, Watermarking is subphylum of information secrecy which can be applied in order to embed watermark into image in for authentication or ownership. Unlike steganography, the receiver doesn't necessarily need to receive all of the bits which contain watermark. Instead, the embedded data is expected to be desirably resistant against the attacks designed and performed in order to remove the watermark without spoiling the quality.

By and large, three elements interfere with information secrecy systems: capacity, security and robustness and usually when one of them improves the other would descend. As to the steganographic methods, capacity and security are mainly significant, but robustness is the most important element in watermarking methods. Images used for data embedding are called cover and those obtained by placing the massage through embedding algorithm are called container.

Most of the steganographic methods which hide their data in a pixel space, apply LSB techniques. Although these methods try to improve the required security for steganography through applying random factors or hidden keys, the investigations performed on statistical components of these images break most of them [3].

Choosing the image format has a considerable effect on steganography system. Uncompressed formats such as BMP provide a large space for steganography but using them is suspicious because of the large volume of extra information. Embedding in the spatial area of unzipped JPEG images is also improper.

Fredric [4] indicated that the hidden massage in the pixel space of an image which was before a JPEG file is discoverable even if it is as little as a single bit [1]. This would be done through performing JPEG compatibility test for each 8x8 block.

Applying Chi-squared test, Westfield and Fitzman have presented an accurate method about a group of steganographic algorithms which use less valuable bits in its embedding one after the other [5]. This method acts based on

generating binary values with same number of occurrence (POV).

In order to overcome the attack presented in [5], Westfield offered the F% algorithm in [6]. In this method, instead of situating the massage in less valuable bits of coefficients, he reduced the real values of the coefficients by one unite and then performed the embedding. F5 applies the encoding matrix, ME= (1, n, k). I e. k bits of massage are embedded in n bit modifiable spaces, in other words, k bits of massage are embedded in LSB bits which belong to n qualified none-zero DCT coefficients. ME = (1, n, k), the encoding matrix means that there is only one non-zero coefficient among the n existing coefficient for embedding of k bits of considered massage, which can be embedded. Therefore, some of the embedded k bits would be immolated to the drop. The shrinkage appears whenever F5 reduces the absolute values of 1 and -1 to produce a zero[7]. The receiver can't distinguish between an unused zero coefficient in steganography and a produced zero through shrinkage so the receiver ignores all of the zero coefficients. Therefore, the transmitter examines if any zero have been produced or not. If a zero was produced, the transmitter omits it by reading one more non-zero coefficient and repeating this process. This omission would be performed whenever a zero is produced.

According to the discussion above, it can be concluded that the main problem of F5-ME embedding process is the shrinkage phenomenon. Shrinkage causes a tangible increase in the number of zeros and a tangible decrease in the number of ones. Another effect of shrinkage is the increase in mean-squared errors (MSEs) of the container image because of the increase in number of zero qualified DCT coefficients (QDCTs). It's clear that zero qualified DCT coefficients preserve their zero value even after counter-qualification. As a result, the remade image would be extremely destructed after conversion of counter-qualified DCT. This discussion explains the relationship between shrinkage and the increase in MSE of the container image[8].

Thus, from the viewpoint of steganography experts the shrinkage phenomenon can easily be revealed by steganographic tools and this shows the presence of secret massage through F5-ME method. In other words, the existence of hidden massage by F5-ME method is very prone to be revealed. In this paper, we introduce a method to reduce the shrinkage phenomenon. This method is based on shrinkage mapping. This map controls the shrinkage rate and as a result, the existence of the covered massage through the new suggested method would be very intangible. The efficiency of the suggested method has been compared with F5 and mod4 algorithms.

Afterward, chapter 2 introduces a suggested method called "Improving F5 Steganography through Shrinkage Mapping". The results of the simulation of this method are presented in chapter 3 and the chapter 4 is the conclusion.

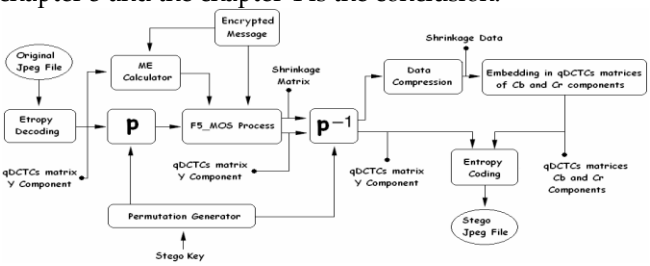

Fig 1.the block diagram of steganography using suggested method (F5-mos)

2 THE SUGGESTED METHOD

In the common F5-ME method the transmitter checks if any zeros have been produced or not, if it had, the transmitter omits the produced zero through reading one more non-zero coefficient and repeating the process because the receiver cannot distinguish between an unused zero coefficient in steganography and a produced zero through a drop. Therefore, the receiver would ignore all of the zero coefficients. Therefore, in common F5-Me method zero coefficients carry no information. Now, the method presented here can remove the shrinkage phenomenon. First, it manipulates the program of the original JPEG file taken by a camera thus the input image is a JPEG file, not a Bitmap one. The Jpeg-read function reads the JPEG file in MATHLAB and provides a MATHLAB structure which contains the arrays of qualified DCT coefficients, qualification tables, Huffman tables and other information.

The common F5-ME method merely manipulates the arrays of the qualified DCT coefficient of Y color and ignores c_b and c_r components. This is because of its big size compared to two other colors. But in the method presented here, c_b and c_r components are also applied in order to record shrinkage points.

2.1 CRYPTOGRAPHY

In this chapter, we suggest a method for controlling shrinkage rate in order to reduce its effects. The method is a new algorithm which is based on the common F5-ME method. This method records the shrinkage situations and embeds the shrinkage information in a similar JPEG file. In other words, it makes a shrinkage map containing shrinkage information and sends it to the receiver through a similar JPEG file. Just like F5-ME, the JPEG reader first decodes the JPEG file and provides a structure which contains the arrays of qualified DCT coefficients, qualification and Huffman tables. Then, the qualified DCT coefficients of Y color component matrix would be changed and the size of the secret massage file and the number of non-zero coefficients in matrix of Y component

qDCTCs would be calculated in order to determine the encoding matrix (ME) for F5 algorithm.

During the embedding process, the suggested method records the shrinkage points and produces a shrinkage matrix with same dimensions of the matrix of Y component qDCTCs. Thus, unlike common F5-ME method, the suggested method produces two matrixes: shrinkage matrix and the matrix of Y component qDCTCs. These two matrixes would be reversely changed in order to produce the main matrix of Y component qDCTCs. Then the changed shrinkage matrix would be compressed using Run-length encoding and a number of other compressing algorithms such as Huffman and mathematical cryptography. Afterward, the shrinkage data in matrixes of c_b and c_r components qDCTCs would be embedded applying a powerful algorithm such as Mod4 or other algorithms. Finally, through entropy algorithm, the resulted qDCTC matrixes for of c_b and c_r components through would be compressed in order to produce a Stego JPEG file. Figure 1 illustrates the embedding stages of the suggested method.

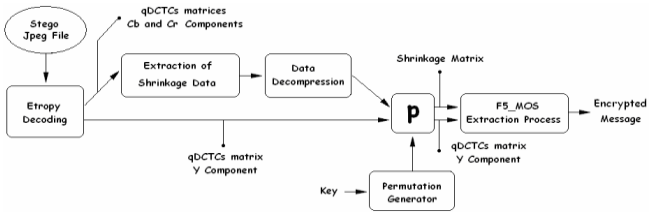

Fig 2 . the block diagram of decryption using suggested method (F5-mos)

2.2 DECRYPTION

In extraction program, the JPEG reader reads the container JPEG file and provides a structure including the matrix of DCT coefficients for Y, c_b and c_r components. The compressed shrinkage data would be extracted from qDCTC matrixes of c_b and c_r components and then, the shrinkage data would be uncompressed in order to produce a shrinkage matrix with same dimensions with the qDCTC matrix of Y component. These two matrixes are changed in order to obtain matrixes in same category which are applied during embedding process. Now, using the shrinkage matrix, the suggested method can recognize (identify) the zero coefficients which contain steganographic information. Finally, the suggested method uses the shrinkage matrix and the matrix of Y component qDCTCs to extract the secret massage. Figure 2 shows the extraction stages of the suggested method.

3 SIMULATION RESULTS

The suggested method in this paper has been tested for different JPEG images and the results are illustrated in table 1 (this suggested method has been performed on the four images included in figure 3).

3.1 EMBEDDING CAPACITY

For a considered image in F5-ME, the embedding capacity differs from one massage to another. This is caused by the appeared shrinkage during embedding process. The shrinkage rate for the considered image also varies depending on the applied change and the embedded massage. The shrinkage would increase the number of qualified DCT coefficients (qDCTCs) and as a result, the embedding capacity would decrease. Therefore, as a result of the shrinkage problem, there is no accurate capacity in F5-ME condition; instead, an approximate value of maximum capacities would be calculated unto bpc sentences using bpc2 relation. This relation considers the shrinkage probability during embedding process and the number of qDCTC ones which reduce to zero after this process.

$$bpc2 = ((\text{Nonzero qDCTCs} - (\text{Ones qDCTCs}/2))*(2/3)) / \text{Nonzero qDCTCs}$$

In the relation above (bcp2), when ME= (1, 2, 3), we would consider that 50% of the one coefficients have been reduced to zero after embedding process. As a result, these reduced ones (zeros) carry no data. Thus, they should be subtracted from the total number of non-zero coefficients.

As to the suggested method, as a result of shrinkage matrix, all original non-zero coefficients can carry the embedded data even if some of them (ones) had been reduced to zero. Therefore, there is no need to subtract them from the number of original non-zero coefficients because all of the have been considered. But, since the c_r and c_b have been used, the non-zero coefficients of these two matrixes must be also applied in order to calculate the embedding capacity. Thus, the following formula is obtained for the calculation of embedding capacity for the suggested method.

Suggested bpc= [(non-zero qdcts y).2/3] / [non-zero qdcts $y+n.z.c_b+n.z.c_y$]

In addition to the operation of the suggested method in four mentioned images, the foresaid method was performed on 60 other images in order to understand its embedding capacity in a better way and the resulted diagram is illustrated in figure 4.

Fig 3. the applied images for embedding information

		MSE	PSNR [DB]	Capacity [bits]
Image1	Proposed	2.1243	44.8586	0.5781
	Mod4	2.1863	44.7334	0.2514
	F5-ME	3.778	42.3582	0.5301
Image2	Proposed	2.6448	43.9069	0.5816
	Mod4	3.27	42.985	0.2664
	F5-ME	5.2002	40.9706	0.5423
Image3	Proposed	2.0817	44.9466	0.5565
	Mod4	1.8503	45.458	0.2369
	F5-ME	3.6728	42.4808	0.5223
Image4	Proposed	1.7263	45.7596	0.5643
	Mod4	1.4658	46.47	0.2441
	F5-ME	3.1157	43.1953	0.5245

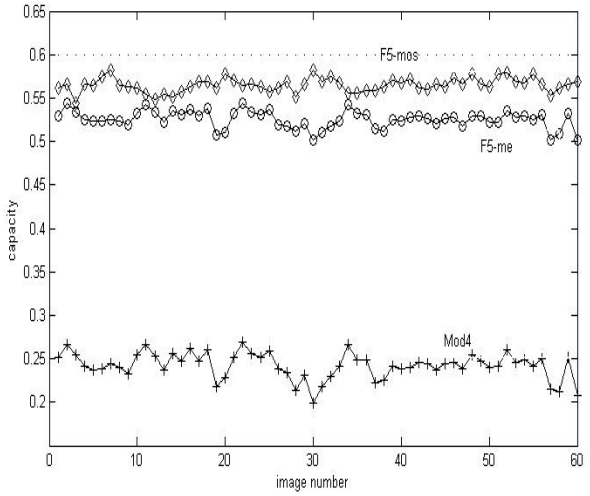

Fig 4. Capacity of 60 images with different methods

3.2 IMAGE QUALITY

In the previous part, the provided capacity by the suggested method (F5-MOS) was compared with the provided capacities by F5-ME and Mod4. The non-observable results of the suggested method would be investigated in this part. Mean-Square Error (MSE) or Pick Signal to Noise Ratio (PSNR) can represent the difference between the original image and the stego one. The pixels of the original image are represented by x_i and $\hat{x}_i$ represents the pixels of stego image. L variant is the maximum light intensity signal. Thus, as to suggested condition of y component (Gray Scale), L=225.

$$\frac{1}{N}\sum_{i=1}^{N}(X_i - \hat{X}_i)^2 \quad (1)$$

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \quad (2)$$

For each existing image in database, a massage would be applied which is correspondent to maximum capacity in case of using Mod4 method with (1, 1, 1, 1) parameters. Thus this would be the biggest massage which can be embedded in its correspondent image applying M4 (1, 1, 1, 1). The provided massage would be embedded in its correspondent image using three different methods, Mod4 (1, 1, 1, 1), F5-ME, and the suggested method (F5-MOS). Each time, MSE and PSNR would be calculated for the obtained stego image. This would be repeated for all four existing images in database (figure 3). Table 1 shows the obtained value of MSE and PSNR for each method. Finally, the average MSE and PSNR values would be calculated for the whole set. Table 2 illustrates the obtained average values.

According to the table above, it is observed that the embedded through data is far less tangible then the data embedded through F5-ME, but its intangibility is almost similar to the data embedded through M4 (1, 1, 1, 1). This improvement in intangibility in the suggested method is caused by application of shrinkage mapping which minimizes the produced zero coefficients.

Therefore, the destruction caused by zero coefficients would be minimized as well. This interprets the results illustrated in table 2.

TABLE 1
The comparison between the suggested method and other steganography methods applying JPEG images

TABLE 2
Average values of MSE and PSNR

method	MSE	PSNE
(1 و 1 و 1) M4	1.6598	45.9302
F5-ME	3.0748	43.2526
Suggested method	1.6867	45.8604

4 CONCLUSION

Finally, it was observed that the use of shrinkage map in the suggested method increases the embedding capacity and acceptably hides the existence of the secret massage.

According to this viewpoint, the quality and capacity of the four existing images was firstly calculated through the block diagram of the suggested method and it was concluded that by and large, both image quality and image capacity can't be maximum simultaneously and there is always am exchange between them. This paper

tries to improve these two conditions simultaneously by presenting a new algorithm.

The suggested method records the shrinkages and places them in c_b and c_r matrixes. As a result of using shrinkage matrix, the suggested method provides more image quality and capacity compared to the common F5-ME method.

REFERENCES

[1] Wayner, p., "Disappearing Cryptography", 2nd Edition , *by Elsivier Science (USA)*, 2002.

[2] Anderson, R.J, Petitcolas, F.A.P., "On the Limits of Steganography", *IEEE Journal of Selected Areas in Communications*, Special Issue on Copyright and privacy Protection, Vol. 16(4), pp. 474-481, May 1998.

[3] R.C.Gonzales and R.E Woods ,Digital Image processing ,Addison publishing Co ,1993.

[4] Fridrich, J., Goljan, M., Du, R., "Steganalysis Based on JPEG Compatibility", Proc. *SPIE Multimedia System and Applications IV, Denver* Vol. 4518,pp. 275-280 Colorado, 2001.

[5] Westfeld, A., Pfitzman, A., "Attacks on Steganographic Systems", Proc. *3rd Int'l Information Hiding Workshop , Springer-Verlog, Berlin Heidelberg New York,* , pp. 61-76, 1999.

[6] Westfeld, A., "F5__ A Steganographic Algorithm :High Capacity Despite Better Steganalysis", Proc. *4th Int'l Information Hiding Workshop, Springer-Verlog* Vol.2137, Berlin Heidelberg New York , pp.289-302, 2001.

[7] Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes, *6th Information Hiding Workshop, J. Fridrich (ed), LNCS*, vol. 3200, Springer-Verlag, pp. 67-81, 2004.Determining

[8] New Methodology for Breaking Steganographic Techniques for JPEGs, with M. Goljan and D. Hogea, in Proc. *SPIE Electronic Imaging Santa Clara*, CA, Jan 2003, pp. 143-155.