www.s2is.org
International Journal on Smart Sensing and Intelligent Systems
ISSN 1178-5608

SECURITY METHOD FOR COMBINATION STEGANOGRAPHY ALGORITHMS ON TRANSFORM DOMAIN FOR JPEG IMAGES

Hamdan L. Jaheel and Zou Beiji
School of Information Science and Engineering, Central South University,
Hunan, P.R. China

Submitted: Aug. 6, 2014 ***Accepted: Nov. 3, 2014*** ***Published: Dec. 1, 2014***

Abstract- Steganography is the act of hiding a message inside another message in such a way that can only be detected by its intended recipient. In any communication, security is the most important issue in the world today. It created a lot of data security and steganography algorithms in the past decade, and that worked motivation for our research. In this paper, Security Method for Combination Steganography Algorithms on Transform domain for JPEG images, we have designed a system that will allow the average user to securely transfer secret messages (picture) securely by hiding them in JPEG image file using local characteristics within the image. This paper is a combination of two steganography algorithms, which provide a strong backbone for its security. The proposed system hides the image unrevealed manner through the use of steganography algorithms to protect each other, where was used F4 algorithm as a wall to protect outguess01 algorithm. We combine between steganography algorithms (outguess 0.1 algorithm and F4 algorithm) to make use of it to provide more

than level of protection for the secret message (image). When save the secret message (image) within an image by using outguess01 algorithm, Which produces outguess-image, then hide outguess-image within another image by using F4 algorithm, Which produces F4-image(stego image). Adopt the principle of camouflage and deception to hide image gives another level of safety for secret Image. Good selection of size and type images used in the process of concealment that contributed to the success of the process of embedded and retrieval of hidden images. Results proved after calculating the capacity and PSNR for images that a good and acceptable steganography scheme. The model presented here is based on JPEG images.

Index terms*:* Transform domain technique, OutGuess0.1 algorithm, F4 algorithm, peak-signal-to-noise ratio (PSNR).

I. INTRODUCTION

Steganography word comes from the Greek Steganos, which mean covered or secret and –graph mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography refer to the act and science of hiding communication, where the hidden information presented cannot be detected [1] the secret information is encoded in a manner such that makes it difficult detect hidden information. Paired with existing communication methods, steganography can be used to carry out hidden exchanges [2,3].

Digital image steganography, as a means of secret communication, aims to transfer a large amount of secret message, relative to the size of the cover image, communication between the parties. Additionally, it aims to avoid the suspicion of non-communicating entities of this type of communication. Basically, cover object steganography may be of many types like Audio, Video, image etc. Image Steganography is very popular because of the popularity of digital image transmission over the internet using the redundancy to hide secret message in digital image by steganography [4, 5]. A steganographic system has two main aspects: steganographic capacity and imperceptible. However, these two characteristics are contrasted with each other. Moreover, the steganographic capacity is quite difficult to increase it and maintain the a steganographic system imperceptible simultaneously .

The security steganographic system is based on the classic secret encoding system. An example of this type of system is a Roman general, who shaved the head of a slave and tattooed a message on it. After the hair grows again, he sent the slave to the delivery of the message hidden now. Despite such a system might work for a time, it is easy enough to shave the heads of all the people passing by to check for hidden messages in the end, the failure of such a steganographic system.

Modern steganography is being undetectable unless confidential information which is secret key known [6]. Steganography to remain undiscovered, must be kept secret the unmodified cover medium, because if it is exposed into a comparison between the cover and stego media immediately detect changes. Information theory allows us to be even more specific on what it means for a system to be perfectly secure. Suggests Christian Cachin a model of information theory for steganography that considers the security of steganographic systems against passive eavesdroppers [8]. In this model, he assumes that the enemy has comprehensive knowledge of the encoding system but the secret key Unknown. Devise a model for the probability distribution PC of all possible cover media and PS of all possible stego media. The enemy can then use the theory of detection to decide between the hypothesis C (that a message contains no hidden information) and hypothesis S (that a message carries hidden content). There is a system completely safe if no decision rule exists that could lead better than random guessing.

Mainly, steganographic communication senders and receivers depends on agreement on steganographic system and the shared secret key that specified how the secret message is encoded in the average cover. To send a secret message, for example, Alice creates a new image with a digital camera. Alice provides the steganographic model with her shared secret and her message. steganography system uses the shared secret to specify how the concealed message should be encoded in the redundant bits. The output is a stego image that Alice sends to Bob. When Bob receives the image, uses the shared key and they agreed on steganographic model to retrieve the secret message [9, 10].

II. OVERVIEW

When you work with images larger than a little deeper, Images tends to become very large to transfer across s standard Internet connection. In order to view an image within a reasonable period of time, must be techniques Incorporated to reduce the size of image file. These Techniques makes use of mathematical equations to analyze and condense the image data, resulting size of file is small, this process is known as compression [3].

In images there are two types of compression: lossy and lossless compression [3]. Compression plays mainly role in choosing which steganographic algorithm to use.

Lossy compression techniques lead to a smaller image file, but it increases the likelihood to be an integral part of The message may be lost, partly due to the fact that excess Image data will be deleted . Lossless compression though, keeps the original digital image intact without the chance of lost, although is does not compress the image to such a small file size.

To compress an image into JPEG format, the RGB colour representation is first converted to a YUV representation. In this representation the Y component corresponds to the luminance (or brightness) and the U and V components stand for chrominance (or color) [15]. According to research the human eye is more sensitive to changes in the brightness (luminance) of a pixel than to changes in its colour [14]. This fact is exploited by the JPEG compression by down sampling the colour data to reduce the size of the file. The colour components (U and V) are halved in horizontal and vertical directions, thus decreasing the file size by a factor of 2 [15].

The next step is the actual transformation of the image. For JPEG, the Discrete Cosine Transform (DCT) is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of “spreading” the location of the pixel values over part of the image [14] .The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block.

The next step is the quantization phase of the compression. Here another biological property of the human eye is exploited: The human eye is fairly good at spotting small differences in brightness over a relatively large area, but not so well as to distinguish between different strengths in high frequency brightness. This means that the strength of higher frequencies can be diminished, without changing the appearance of the image. JPEG does this by dividing all the values in a block by a quantization coefficient. The results are rounded to integer values and the coefficients are encoded using Huffman coding to further reduce the size [15].

III. TRANSFORM DOMAIN TECHNIQUE

Originally modification techniques are easy ways to include the information, but they are highly vulnerable to even small adjustments cover. An attacker can simply apply signal processing techniques for the destruction of confidential information completely . In many cases, even small changes resulting out of lossy compression systems yield to total loss of information.

It has been observed in the development of a steganographic system that conceal information in the frequency domain of the signal can be more powerful than the concealing rules working in time domain technique . Steganographic stronger systems known today actually work in a kind of transform domain.

Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attack, such as compression, cropping, and some image processing, then the LSB approach.

Conceal information by spatial domain, it may be subjected to the damages if the image subject to any image processing technique like compression, cropping etc. To overcome this problem concealed the information in frequency domain such that the confidentiality information is concealed on the significant frequency values while being deleted the high-frequency part. First implement transformations to the image, and then data is to be copy changing the values of the transformation coefficients accordingly. There are mainly three transformation techniques Fast Fourier Transform (FFT) Steganography, Discrete Wavelet Transform (DWT) Steganography and Discrete Cosine Transform (DCT) Steganography. The following point explains DCT domain.

IV. DISCRETE COSINE TRANSFORM (DCT)

In this technique two dimensional DCT is used for transformation of cover image [13,14]. DCT is derived from the FFT, however, it requires fewer multiplications than the FFT since it works only with real numbers. Also, the DCT produces fewer significant coefficients in its result, which leads to greater compression. Hence DCT is the popular technique in the field of steganography[15],If after DCT transformation, quantization step is also taken as in Joint Photographic Experts Group (JPEG) compression [16] then it becomes robust to JPEG compression and this technique is called as JPEG steganography [17].

For each color component, the JPEG image format uses a discrete cosine transform (DCT) to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients *F(u, v)* of an 8 × 8 block of image pixels *f(x, y)* is given by Eq (1):

Fig. 1: set of images that we used in experimental results.

$$f\ \ u,v\ \ = \frac{1}{4}\ C\ \ u\ \ C\ \ v\ \ \ {}_{x=0}^{7}\ \ {}_{y=0}^{7} f\ \ x,y\ \ \cos\frac{(2x+1)\pi u}{16} * cos\frac{2y+1\ \ \pi v}{16} \qquad (1)$$

For x=0,….,7 and y=0,…,7

$$wherC\ \ k\ \ = \begin{matrix} 1\ \ \overline{2}, & for\ k=0 \\ 1\ \ , & otherwise \end{matrix}$$

Afterwards, the following operation quantizes the coefficients as in Eq (2):

$$Q\ \ u,v\ \ = \frac{F(u,v)}{Q(u,v)} \qquad (2)$$

Where Q(u,v) is a 64-element quantization table. We can use the least-significant bits of the quantized DCT coefficients as redundant bits in which to embed the hidden message. The modification of a single DCT coefficient affects all 64 image pixels.

Before starting the process of embedding, in JPEG image all 8 x 8 blocks are converted to the frequency domain using DCT and then uses DCT to transform each block into DCT coefficients. In a request for the values that will be displayed whole numbers, each 8x8 block is quantized according to a Quantization Table. Two types of coefficient could be seen on every 8*8 block: DC and AC. It is known that value at the top left of each 8*8 block refer to DC coefficient. It contains the mean value of all the other coefficients in the block, referred to as the AC coefficients. DC coefficients give a good estimate of the level of detail in the block because it is very important for each block. Therefore cannot manipulating or changing the value coefficients DC because it will lead to change many of the values of the AC coefficients, this will lead to a visual discrepancy when the image is converted back to the spatial domain and viewed normally.

For this reason, the JSteg algorithm does not embed message data over any of the DC coefficients for every block. And also, the algorithm doesn't permit embedding on any AC coefficient equal to 0 or 1 [18].An example of an 8x8 DCT block is shown in Fig.2

352	-5	-8	-6	-4	-1	-3	1
-1	-3	-1	0	0	-1	1	0
7	0	-1	3	0	-2	-2	-2
4	2	1	1	2	0	-1	1
-3	-1	0	-1	0	0	0	0
-1	1	-1	-1	0	1	-1	0
-2	-2	0	0	1	1	-1	0
0	-1	-1	0	0	-1	0	1

Fig2: An example of an 8x8 sub-block of DCT coefficients.

V.OUTGESS0.1 ALGORITHM

Outgess 0.1 preserves statistics based on frequency counts. As a result, statistical Outguess 0.1 preserves statistics based on frequency counts, on this basis, it is not possible to detect steganographic contents. Before starting the process of concealing data, Outquess can be determined the maximum of the message size that we want be hiding it in another message, while still being able to maintain statistics based on frequency counts. Because the chi-square attack is based on analyzing first-order statistics of the stego image, based on this it cannot detect concealed messages that using an algorithm Outquess [19].

Algorithm OutGuess 0.1 represents a process of concealment through a mixture of both the randomized Hide & Seek algorithm and the JSteg algorithm. Firstly, step is to convert the image to the DCT domain. Then, the coefficients are shuffled into a seemingly random order using a PRNG according to a seed. Then, message data are embedded by using the same technique as for JSteg .Where JPEG image all 8 x 8 blocks are converted to the frequency domain using DCT and then uses DCT to transform each block into DCT coefficients. In a request for the values that will be displayed whole numbers, each 8x8 block is quantized according to a Quantization Table. Two types of coefficient could be seen on every 8*8 block: DC and AC. It is known that value at the top left of each 8*8 block refer to DC coefficient. Before finally inverse the shuffle such that the coefficients are back in the correct positions. Then, converted back the image in the spatial domain and thus the stegogrammes is produced

[18]. The algorithm still avoids embedding within the DC coefficient, and any AC coefficient equal to either 1 or 0. The first version of OutGuess, designed by Neils Provos [10].

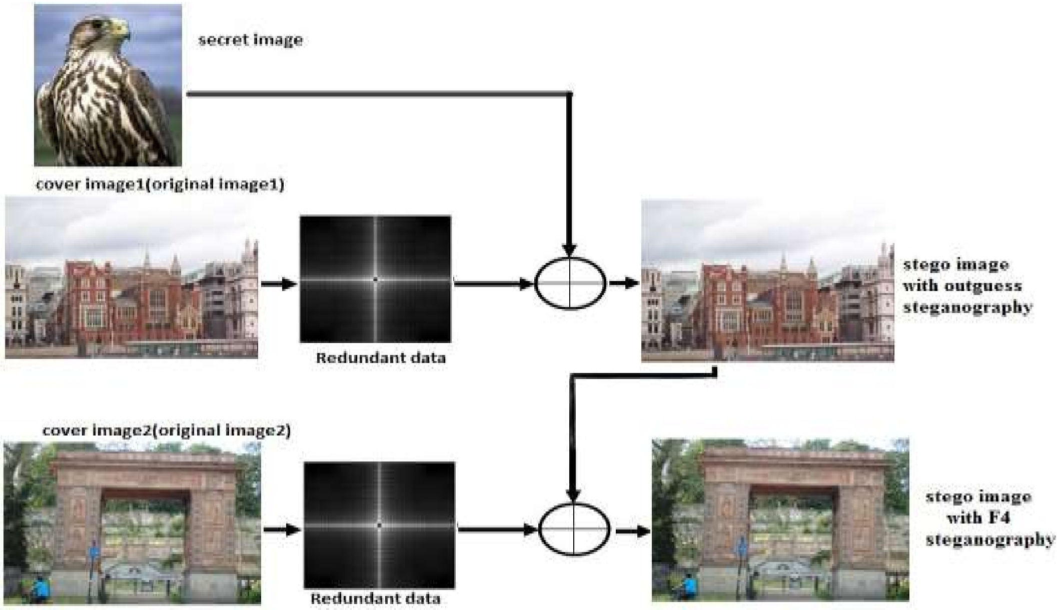
secret image
cover image1(original image1)
Redundant data
stego image with outguess steganography
cover image2(original image2)
Redundant data
stego image with F4 steganography

Fig. 4: Diagram explains the proposed method.

VI. F4 ALGORITHM

Two the weaknesses of algorithm F3 are canceled in one fell swoop by using an algorithm F4, by mapping negative coefficients to the steganographic value, where even-negative coefficients = steganographic 1, odd-negative coefficients = 0, even-positive coefficients = 0 (as with JSteg and F3), and, odd-positive coefficients = 1 [20] . More simply put, this means if embed a 0 in a DCT coefficient equal to -3, the result will remain -3, whereas it would have been modified to -2 using F3. This means that the bit-flips now occur with roughly the same probability.

The following action when you conceal the secret message data according to the algorithm F4 during the quantize DCT coefficients. F4 not embed on the DC coefficients or any AC coefficient equal to zero. Again, the DC coefficient is the same for both image (a) and image (b) this means that the algorithm correctly stay away concealing on these values. In addition, that the second AC coefficient in the image (a) equal 7 is correctly decrement to 6 when embedding a 0.

Similarly, the third AC coefficient equal -5 increments to -4 when an equal 1 is embedded. This is at the bit-flips denoted in Figure 3[18].

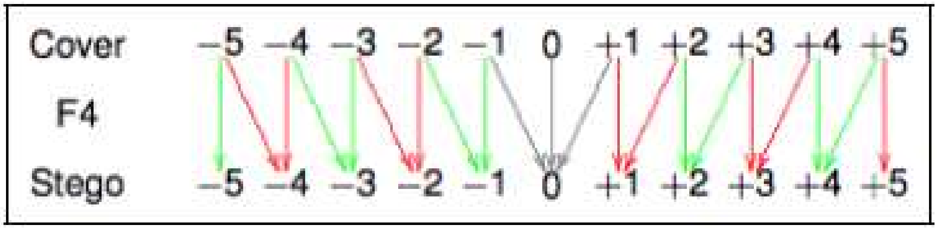

Fig 3: The expected bit flips from the F4 algorithm [21]

VII. PROPOSED METHOD

In this paper, propose a manner for conceal or hide large volumes of data in images while incurring minimal perceptual degradation. The embedded data can be recovered successfully, without any errors, after operations such as decompression, additive noise, and image tampering. We are merging between steganography algorithms OutGuess algorithm and F4 algorithm, to provide more than level of protection for the hidden message, Where based on the principle of camouflage and deception, where the secret image will be saved first within an image by using an OutGuess algorithm (result stego-image1 outguess image), then save stego image1(OutGuess image) within another image by using an F4 algorithm (that result stego-imag2). This hiding manner gives another level of safety for secret Image, through benefit from the characteristics and features for each algorithm, that gives strong system from difficult detect it. Illustrate the encoding method in fig 5.

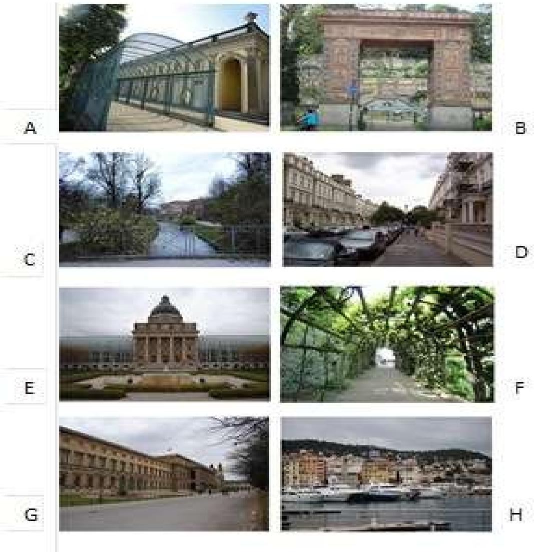

Fig. 5: set of stego images with encoding F4 algorithm

A.Embedding algorithm

```
Input: cover image1, cover image2, secret image1(message1), secret image2(message2)
Step1: read cover image1. JPEG
A. JPEG partitions a cover image1 into non overlapping blocks of 8*8 pixels
B. Calculate DCT coefficient for each block
C. Quantize the coefficients
Step2: Step6:hiding process by using Outguess algorithm
While left to embed do
 Get pseudo random DCT coefficient from cover image2
      If DCT ≠0, DCT ≠1 & DCT ≠ -1 then
       Get LSB from message1
    Replace DCT LSB with message1 bit
End (if)
End (while)
Step7:   calculate message capacity
Step8:   Writ JPEG image by de-quantize and take inverse DCT to obtain stego image1.
        Secret image2 (message)= stego image1
Step5: Read cover image2.JPEG
A. JPEG partitions a cover image2 into non overlapping blocks of 8*8 pixels
B.  Calculate DCT coefficient for each block
C.  Quantize the coefficients
Step6: hiding process by using F4 algorithm
      for i = 1, ..., l(m) do
          p←   di
         while p = DC or p = 0 do
             p = next DCT coefficient from d
         end while
      P←   absolute(pi)
          if P = mi and P > 0 then
            P←   P + 1
             absolute(di)   P
           else if P 6= mi and P < 0 then
            P←   P + 1
             absolute(di)   P
        end if
        if di = 0 then
           next mi = mi
        end if
       Ci←   pi
      end for
Step7: calculate message capacity
Step8: Writ JPEG image by de-quantize and take inverse DCT to obtain stego image2.
```

After the implementation of this algorithm in Matlab 7.6 program got the results shown in Figure (3) that illustrate new method use a unique combination of steganographic methods in the frequency domain. Where first hidden an image within an image by using outguess algorithm and then hidden the stego image with outguess inside another image by using F4 algorithm.

B. Extracting algorithm

Input: stego image2

```
Step1: read Stego image2.JPEG
          A. JPEG partitions Stego image2 into non overlapping blocks of 8*8 pixels
          B. Calculate DCT coefficient for each block
          C. Quantize the coefficients
          D. Calculate message capacity
Step2: Extracting process by using F4 algorithm
      for i = 1, ..., l(m) do
        p ← di
      while p = DC or p = 0 do
         p = next DCT coefficient from d
      end while
       P ← absolute(pi)
      if P = mi and P > 0 then
      mi ← absolute(pi) - 1
      else if P 6= mi and P < 0 then
      mi ← absolute(pi) + 1
      end if
     Step 3: Writ JPEG image by de-quantize and take inverse DCT to obtain secret image2
     Stego image1= Secret image2
     Step4: Read Stego image1.JPEG
               JPEG partitions Stego image1 into non overlapping blocks of 8*8 pixels
     B. Calculate DCT coefficient for each block
     C. Quantize the coefficients
     D. calculate message capacity.

Step5: Extracting process by using Outguess algorithm
While left to embed do
    A. Get pseudo random DCT coefficient from Stego image1
    B. If DCT ≠0, DCT ≠1 & DCT ≠ -1 then
    C. Get LSB from the message
    D. Replace DCT LSB with message bit
End (if)
End (while)
Step6: Writ JPEG image by de-quantize and take inverse DCT to obtain secret image1.
```

After the implementation of this algorithm in Matlab 7.6 program got the results shown in Fig6

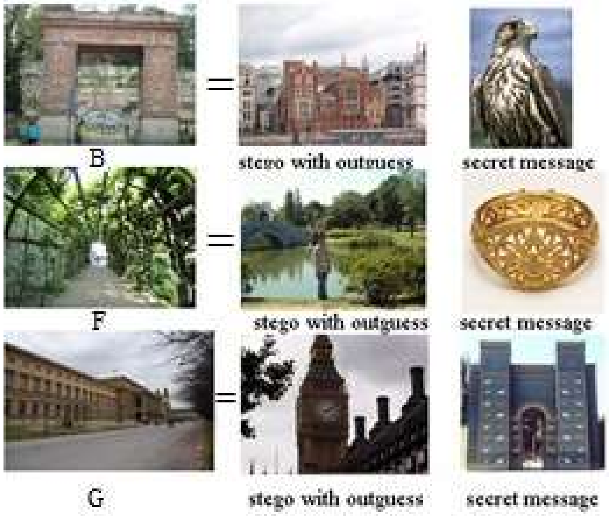

Fig. 6: Illustrate extract images with the decoding F4 algorithm.

VIII. EXPERIMENTAL AND RESULTS

During the concealment process information JPEG compression results in stego image with a high level of Invisibility, since the embedding happens in Transform domain. JPEG image file is the most widely used through the Internet and a small image size because of the compression, thus making it the least suspicious algorithm to use. However, the process of the compression is a very mathematical process, making it difficult to implement. The JPEG image file format is suitable for applications of steganography, especially for images that have send through the Internet.

Experiments implemented on a set of images that downloaded from images database at Washington university [22] (more than 500 images from type JPEG) and also some images from the special camera.

A. Embedding Capacity

It is the maximum size of the secret data that can be embedded in the cover image without deteriorating the integrity of the cover image. It can be represented in bytes or Bit Per Pixel(bpp),The calculated explain in equation 3.

$$Capacity = (X*Y)/64 \quad * b * (n - 15) \qquad (3)$$

In this equation, X and Y are the dimensions of the cover image. By dividing the product of X, Y by 64, the number of 8*8 blocks is achieved. During data embedding process, no data are embedded in the last 15 coefficients, so the term (n-15) is used here, and in each coefficient b bits of data will be embedded.

B. Mean Square Error (MSE)

It is defined as the square of error between cover image and stego-image [23]. The distortion in the image can be measured using MSE and is calculated using Equation 3.

$$MSE = \frac{1}{MN} \overset{M}{\underset{x=1}{}} \overset{N}{\underset{y=1}{}} \quad S_{xy} - C_{xy} \quad ^{2}$$

(4)

Where x and y are the image coordinates, S_{xy} is the generated stego-image and C_{xy} is the cover image.

M*N is Size of an Image.

Peak Signal Noise Ratio (PSNR)

It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. It measures the statistical difference between the cover and stego-image, is calculated using Equation 4.

$$PSNR = 10 \log 10 \ \frac{C_{max}^{2}}{MSE} \qquad (5)$$

Where C_{max}^{2} holds the maximum value in the image. PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40 dB and above. In this paper combine between steganography algorithms outguess algorithm and F4 algorithm, We use the F4 algorithm to add another level of protection to prevent detection the secret message (image), which has been hidden inside another image by using an outguess algorithm. Where the secret message (image) has been saved within an image by using outguess algorithm, then save outguess-image within another image by using F4 algorithm.

The capacity calculates two times to get the hidden image. The first time for outguess algorithm and the second time for F4 algorithm, and this is another level of safety for secret image. All the results of the PSNR, calculated after sending the final result from Stego-image via e-mail to another computer, and retrieve the hidden message (image), then calculates the PSNR that was between (50-65)db and this ratio is considered very good and acceptable steganography system, Figure (4) illustrate for some of encoding processes, and as shown in the following table(2) that explain PSNR & capacity for some encoding processes.

Table 2 show that the Capacity of embedded data size and PSNR of our proposed technique is better than proposed technique in reference [24], and using images with size 512*512 in this comparison**.**

Depending on the result of the comparison, we find that the proposed method is good and acceptable and safe steganography scheme.

TABLE I.

EXPLAIN PSNR & CAPACITY FOR SOME ENCODING PROCESSES

Encoding process	Image	Capacity	PSNR
A	F4 Stego image	2618400	50.3847
B	F4 Stego image	4919984	60.3372
C	F4 Stego image	2994176	55.9085
D	F4 Stego image	1187592	52.83
E	F4 Stego image	1157088	53.3924
F	F4 Stego image	460448	62.4764
G	F4 Stego image	1249888	59.0604
H	F4 Stego image	1047288	58.8402

TABLEII.
COMPARISON BETWEEN OUR PROPOSED METHOD WITH THE RESULTS of TECHNIQUE IN REFERENCE [24]

Cover image	Previous results	**proposed method**

	Capacity embedded data size (bits)	PSNR (dB)	capacity embedded data size (bits)	PSNR (dB)
Lena	**35304**	**37.81**	**50608**	**47.8680**
Barbara	**43641**	**36.21**	**50632**	**50.029**
Mandrill	**61647**	**32.11**	**50640**	**45.2824**
Airplane	**36782**	**38.43**	**82224**	**46.3082**
Boat	**38780**	**37.36**	**82408**	**46.9964**
Goldhill	**46685**	**35.83**	**82304**	**45.0472**
Peppers	**36753**	**36.47**	**82288**	**44.45**
Zelda	**31374**	**39.20**	**82272**	**46.3624**

IX. CONCLUSION

The Digital Image Steganography system allows an average user to securely transfer messages by hiding it in a digital image file. A combination of Steganography algorithms (outguess algorithms and F4 algorithms) provides a strong backbone for its security. Digital Image Steganography system features techniques for hiding messages in a digital image file . In this paper, we combine between steganographic algorithms outguess 0.1 algorithm and F4 algorithm, to make benefit from the characteristics and features for each algorithms together. We use F4 algorithm to add another level of protection to prevent detection the secret message (image), which protect the secret message, when save it within an image by using outguess algorithm, Which produces outguess-image, then hide outguess-image within another image by using F4 algorithm, Which produces F4-image(stego image). Through the use of deception and camouflage to add another level protection for secret Image. The obtained experimental results by calculating the capacity and by the results of the PSNR that was between (50-65)db, and depending on the characteristics of algorithms used in this paper, we say that the resulting system is a successful system and acceptable and safe for the secret message.

REFERENCES

[1] M. Ramkumar & A.N. Akansu. "Some Design Issues For Robust Data hiding Systems", Conference Record of the Thirty-Third Asilomar Conference on Signals, Systems, and Computers, 1528 – 1532, 1999

[2] N.F. Johnson, S. Jajodia, "Staganalysis: The Investigation of Hiding Information", IEEE, pp. 113-116, 1998.

[3] R.Popa,"An Analysis of Steganographic System", The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.

[4] Kurak, C., and J. McHughes, "A Cautionary Note On Image Downgrading," in IEEEComputer Security Applications Conference 1992, Proceedings, IEEE Press, 1992, pp.153-159.

[5] Johnson, N. F., and S. Jajodia, "Exploring Steganography Seeing the Unseen, IEEE Computer , vol. 31, no. 2, 1998, pp. 26-34.

[6] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," *Proc. IEEE*, vol. 87, no. 7, 1999, pp. 1062–1078.

[7] Thomas Mittelholzer, An information-theoretic approach to steganography and watermarking,Information Hiding, pp.1-16,2006.

[8] C. Cachin, An Information-Theoretic Model for Steganography, Lecture Notes in Computer Science, vol.1525, pp.306-318, 1998

[9] A.Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," Proc. Information Hiding—3rd Int'l Workshop, Springer Verlag, 1999, pp. 61–76.

[10] N. Provos, "Defending Against Statistical Steganalysis," In Proceedings of USENIX Security Symposium, 2001, pp. 323–335.

[11] Bender, W., D. Gruhl, and N. Morimoto, “Techniques for data hiding”, IBM Systems Journal, vol. 35, no. 34, 1996, pp. 131-336.

[12] M¨oller, S., A. Pitzmann, and I. Stirand, “Computer Based Steganography How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best, in Information Hiding” First international Workshop, Proceedings , Springer, 1996, pp. 7-21.

[13] Cox, I., et al. , "A Secure, Robust Watermark for Multimedia," in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, pp. 185-206.

[14] O. Runaidh, J. J. K., F. M. Boland, and O. Sinnen, "Watermarking Digital Images for Copyright Protection, , Image and Signal Processing, Aug. 1996, vol. 143, pp. 250–256.

[15] J.R. Hernandez, M. Amado, & F. PerezGonzalez, “DCTDomain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure”, IEEE Trans. Image Processing, 9, Jan. 2000, 55-68.

[16] Wallace, G. K., The JPEG Still Picture Compression Standard, Communications of the ACM, vol. 34, no. 4, 1991, pp. 30-44.

[17] J.J. Eggers, R. Bauml and B. Girod, “A communications approach to image steganography”, Proceedings of SPIE, vol.4675, pp.26-37, 2002.

[18] Philip Bateman and Dr. Hans “Image Steganography and Steganalysis”, M.S. thesis, Department of Computing Faculty of Engineering and Physical Sciences, University of Surrey Guildford Surrey, United Kingdom,2008.

[19] Fridrich J., Goljan M., and Hogea D., “Attacking the OutGuess”, *Proc.ACM Workshop Multimedia and Security*, 2002.

[20] A. Westfeld. "F5 - A Steganographic Algorithm: High Capacity Despite Better Steganalysis", Lecture Notes in Computer Science, vol. 2137, pp. 289-302, 2001.

[21] H. G. Schaathun. "CSM25: Secure Information Hiding", Lecture Notes, University of Surrey, UK, 2008.

[22] http;//www.cs.washington.eduresearchimagedatabasegroundtruth_tars.for.download

[23] Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, “Steganography: Dct Coefficient Replacement Method andCompare With Jsteg Algorithm” International Journal of Computer and Electrical Engineering, Vol. 4, No. 4, August 2012.

[24] Hideki Noda, Michiharu Niimi, and Eiji Kawaguchi, “High performance JPEG steganographyusing quantization index modulation in DCT domain” Pattern Recognition Letters 27, (2006). Issue 5, 455 – 461

[25] Yanmin LUO, Peizhong LIU and Minghong LIAO, An artificial immune network clustering algorithm for mangroves remote sensing, International Journal on Smart Sensing and Intelligent Systems, VOL. 7, NO. 1, pp. 116 – 134, 2014.

[26] Daode Zhang et al., Research on chips’ defect extraction based on image-matching, International Journal on Smart Sensing and Intelligent Systems, VOL. 7, NO. 1, pp.321 – 336, 2014.