Secure Genetic Based Image Steganography System in Frequency Domain

Z. Moghaddasi and Azizah Bt Abdul Manaf

***Abstract*—Steganography is a hiding system that conceals the information in a way only the sender and the recipient know about its existence. Various steganography methods developed to cover different objectives of steganography applications. All these objectives support the main goal of steganography that is undetectability. In this paper a DCT based steganography system is proposed to embed information in 4th bits of DCT coefficients and optimize quality of the obtained stego-images applying genetic algorithm that looks for the best position for embedding. The main idea is derived from SSB-4 method which embeds the message in more significant bits to be more resistant against various steganalysis methods. The experimental results show that the proposed method enhances the imperceptibility and undetectability of the stego-images and is resistant against some steganalysis techniques such as chi-square attack.**

***Index Terms*—Discrete cosine transform, genetic algorithm, steganography, stego-image.**

I. Introduction

In recent years, people are tending toward developing methods for inventive secret communication. One of these methods that become more popular between others is steganography. The history of steganography shows that this method is not new and used in different approaches from the past times. The word steganography itself has been derived from Greek and means "covered writing" [1]. In contrast with cryptography that hides the content of message, steganography is about concealing existence of message in such a way no one, except the sender and intended recipient suspects its existence.

Every system has its own primary and key characteristics in which distinguish that system from others. Steganography system also has three main properties which are imperceptibility, capacity, and robustness [2]. In this paper a genetic based steganography method is proposed to find the best position for hiding message so it increases imperceptibility and undetectability of the obtained image to resist against steganalytic methods such as statistical attacks. This paper is organized as follows:

First image steganography and its various methods are introduced. Then some measurements required for evaluating results of the proposed method are described. After that the proposed method and its experimental results are presented.

II. Image Steganography

Moreover, steganography can be defined as a method of securing data by concealing the contents in another media (carrier or cover object) in which it is stored or transmitted. The carrier could be an image, audio or video file and the secret message which is called payload can also be any digital medium such as text, image, audio, or a video. The word stego-object or steganogram is also used for the media along with the hidden message. The main goal of steganography is to hide data inside other "harmless" media; so an attacker should not be able to find out the hidden message that is embedded in the steganogram.

Images compared to other types of media are the most widely type of carrier used in steganography. This is because information can be hidden in images in different ways without perceptible impact to the carriers and also can be taken advantages of restricted power in human visual system (HVS) [3]. Almost any kind of file formats which is encoded into a bit stream can be concealed in a digital image. The steganographic methods are categorized into two general groups including spatial domain and frequency domain.

A. Special Domain Embedding

In spatial domain techniques the secret message and the carrier are modified in the spatial domain of an image that means embedding at the level of Least Significant Bits [1]. This technique has high capacity embedding and does not make any significant changes to the carrier, so the human eyes are not able to detect the hidden message. Also when the security has the high priority between other factors, LSBs uses a stego-key or the secret message is embedded in noisy areas. The noisy areas refer to the areas where the range of color varies widely to lead into least perceptibility [4]. Several techniques developed in this area such as Least Significant Bit substitution (LSB), cover regions & parity bits, and Pseudo-random permutation [5].

Although spatial domain techniques are very simple, they have a lot of weaknesses. One of them is that the format of images which are suitable for spatial domain steganography is lossless and consequently these methods are usually dependent on the image format. The dependency to image format made spatial domain techniques vulnerable to attacks such as image manipulation and it is due to leaving statistical evidences behind in the modified image [4]. A trivial conversion between image formats for example from GIF to JPEG which is a lossy compression image format can change the embedded message's content [3].

B. Frequency Domain Embedding

It is shown that embedding information in frequency domain of a signal is more robust than embedding it in the spatial domain. This leads to developing more robust techniques which function in some sort of transform domain.

Transform domain methods by embedding secret message

Manuscript received October 13, 2012; revised November 24, 2012

The authors are with Advanced Informatics School, University Technology Malaysia, 54100 Kuala Lumpur, Malaysia (e-mail: mzahra2@live.utm.my, azizah07@ic.utm.my)

in significant areas of the carriers makes them more resistant than spatial domain methods against attacks such as compression, cropping, statistics, etc. There are many frequency domain methods such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Due to using DCT in this paper, this technique is described in this section briefly.

DCT is the most popular block-based transform. It decorrelates the image data and then each transformed coefficient can be encoded freely without missing compression efficiency [6]. DCT is the basis for most of the image and video compression algorithms, especially the image compression standard JPEG in lossy mode and the video compression standards MPEG-1, MPEG-2, MPEG-4, H.263, etc [7].

In DCT-based embedding method, first the image is transformed to high and low frequency sub-bands. Then the message bits are embedded into the coefficients. The advantage of this method is making least distortion and modification in statistical properties of an image [4]. The formula used for calculating two-dimensional DCT is expressed in (1):

$$S(u,v) = \frac{2}{N} C(u)C(v) \times$$

$$\sum_{u=0}^{N-1} \sum_{v=0}^{N-1} s(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right) \quad (1)$$

$$\mathrm{C(k)} = \begin{cases} \frac{1}{\sqrt{2}} & \text{for k} = 0 \\ 1 & \text{otherwise} \end{cases}$$

where u, v = 0, 1, 2, …, N-1. Therefore, frequency domain techniques in comparison with spatial domain techniques improve the robustness and imperceptibility of steganographic algorithms, but instead the capacity will decrease because the message can only be embedded in some regions of the image.

C. Image Quality Assessment

Since the imperceptibility is one of the main goals in steganography, the capability to measure quality of an image is very important in steganographic techniques. There are several techniques to measure quality of the image such as Peak Signal to Noise Ratio (PSNR) [8]. PSNR is based on the comparison between the stego-image and the cover image and is calculated applying (2) and (3):

$$PSNR = 10\, Log_{10}^{\frac{MAX^2}{MSE}}\ dB. \quad (2)$$

where MAX is the maximum pixel value of the image which is 255 for a grayscale image with 8 bits depth. MSE which stands for Mean Square Error is calculated in (3) for an M × N grayscale image:

$$MSE = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |I(i,j) - I'(i,j)|^2. \quad (3)$$

where I, I' are the pixel value of the cover image and stego-image respectively. PSNR applied to evaluate quality of the obtained stego-images, and guarantees that they are unsuspicious. The value of PSNR for the steganographic techniques should be more than 30 decibels (dB) to make sure that the quality of the obtained stego-images is acceptable [9].

D. Chi-Square Attack

Since the embedding process results some changes in the carrier, the attackers can use some approaches to guess the existence of secret message and may also reveal the message itself.

Many of steganalytic systems use statistical features of a steganogram to detect the existence of the secret message. That is because the embedding process leaves some traces in the carrier features and makes the steganogram detectable to the attakers. In other word, the statistical characteristics which are read from the carrier should be same as those read from the stego-object, otherwise the stego-object is not robust against the attacks.

Westfeld, A. *et al*. [10] proposed a statistical attack approach by considering that the secret message modifies the histogram of color frequencies in a special way. They assume that using LSBs of the pixels in an image during embedding message process modifies the distribution of the frequencies. The bits used in the embedding process should be equally distributed to keep the frequencies same.

In their case, they use a test called Chi-square test to understand whether the color frequency distribution matches the distribution obtained from the stego-object. The assumption for a modified image is that there are correlations between the adjacent frequencies so that their value is close to each other [10]. Their test can also be applied for an image which transformed to frequency domain [11]. We apply this attack for evaluating the robustness of our proposed method.

III. The Proposed Method

Since the most steganalysis techniques designed to break steganographic algorithms based on LSB, embedding in more significant bits will make them more resistant against various attacks. Beside this, embedding data in those bits reduces quality of the stego-image and threats its undetectability which is the main goal of steganography. So it is necessary to modify the stego-image to increase its quality.

Our proposed method is based on genetic algorithm which looks for the best position to embed the message in DCT coefficients and optimizes quality of a stego-image. According to this method the message is embedded in 4th bits of nonzero DCT coefficients to resist against most of statistical attacks such as chi-square attack. The format of cover images applied in this method is JPEG due to its small size which makes it most popular image format used in various applications.

Basically, the main idea is derived from SSB-4 algorithm proposed by Rodrigues, J. et al. [12]. SSB-4 combines the spatial domain methods with human visual system features to reduce the difference between the stego-image and the original image. They used more significant bits (4th bits) of the original image to embed the message and then changed 1st, 2nd, 3rd, and 5th bits to obtain the minimum difference with the original image. Their hypothesis was that the difference must be equal or less than four (i.e. ±4) because this amount is imperceptible to human eyes.

After that, Kafri1, N. et al. [9] enhanced the SSB-4 method by using DCT. In their proposed algorithm, they applied SSB-4 method in which the message is embedded in 4th bit of the DCT coefficients and then 1st, 2nd, 3rd, and 5th bits will be changed to get minimum difference between the original value and the value after embedding. They also consider if the difference is equal or less than ±8 the human eyes cannot detect the embedded message and so the quality of the image is not corrupted. In our proposed method this difference reduces by optimizing the stego-image using genetic algorithm. The following steps indicate the proposed approach:

- Step 1: preparing the image

In this step first the cover image is divided into 8 × 8 blocks and every block is converted to DCT using (1). Then the coefficients are quantized based on JPEG algorithm.

- Step 2: embedding process

In this step first every 8 × 8 block of coefficients is converted into a vector. This vector forms the chromosome of our genetic algorithm which consists of 64 genes. The message bits are embedded into 4th bit of every nonzero coefficient included in this vector. Next the genetic algorithm optimizes the embedded chromosome to find the minimum difference between the original chromosome and embedded one.

Equation (4) shows the fitness function for our GA-based method to calculate the difference between the cover image and embedded ones. This function called Mean Absolute Difference (MAD) is applied by Pik-Wah as an image quality indicator for his GA-based watermark algorithm [13]. Milani Fard, A. et al. [14] also combined the Outguess method and MAD, as the genetic algorithm fitness function for improving the quality of their obtained stego-image.

$$\overline{|\delta|} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}|I(x,y) - I'(x,y)|. \qquad (4)$$

where I and I' are the coefficient value of the cover image and stego-image respectively and N is size of the block that is 8 in our case.

Furthermore, the genetic operations applied in this method are crossover and mutation. Crossover is an operation in which two chromosomes are combined together according to a function to produce children for next generation. Mutation also operates only on a single chromosome and changes some portions of that chromosome. As mutation might modify the 4th bits of coefficients and corrupt the embedded data, its function should be designed in such a way to change only 1st, 2nd, 3rd or 5th bits of the coefficients.

- Step 3: constructing the image

After applying the designed genetic algorithm, if the fitness function value is less than determined criteria, the chromosome will be selected as embedded chromosome and is replaced with the original one. After embedding the whole message in the 8 × 8 blocks and replacing them with the original blocks the stego-image is constructed. The whole process is presented in Fig. 1

IV. Implementation

The proposed method was implemented using MATLAB and its toolboxes such as image processing and genetic algorithm & direct search on Microsoft Windows XP. The genetic algorithm functions were customized as required to meet our genetic based scheme. Also a JPEG toolbox for manipulating images in JPEG format was added to MATLAB and applied [15].

```
read cover image
read message file
transform cover image into 8 × 8 DCT blocks
for every 8 × 8 block
  for every nonzero coefficient
    if 4th bit of coefficient is not equal to
    message bit
      Replace 4th bit of coefficient with the
      message bit
    end if
  end for
  initialize population randomly
  evaluate initial population
  repeat
    generate next generation
    select individuals for mating randomly
    exchange parts of individuals by
    crossover
    mutate selected individuals
    keep best individuals from previous
    population
    evaluate new individuals
  until termination criteria satisfied
  replace old coefficients with new ones
end for
construct the stego-image
```

Fig. 1. Process of the proposed method

V. Experimental Results

This section compares the obtained results from the proposed algorithm with DCT and 4th bit method proposed in [9] on 25 grayscale and color images in JPEG format which grouped into five categories relevant to human perception; building, mountain, flower, people, and tree [9].

These results obtained from the cover images with the same size. Then the stego-images and algorithms are compared together through the quality measurement called PSNR. After that the robustness of our proposed system is evaluated through Chi-Square attack and the results are compared with JSTEG algorithm. As JSTEG embeds the message into LSB of DCT coefficients of an image; it is an appropriate steganography system for comparison with the proposed algorithm.

A. Quality Evaluation

As mentioned earlier one of the main goals of a steganography system is imperceptibility. The high imperceptibility means that the quality of the steganogram should be high enough in such a way the human visual system cannot be able to detect even the existence of message in the stego-image [2]. Besides HVS there are also some standard measures to calculate the quality of the steganogram.

In this section PSNR is calculated to evaluate the quality of the proposed method in comparison with DCT and 4th bit method proposed in [9]. Size of embedding message is 40 bytes for all images. The results are average of PSNR values for 5 images in each category which calculated applying two algorithms. Table I shows results of PSNR in grayscale images after embedding the message. As the values illustrate

there is an improvement in PSNR values in the proposed algorithm in all categories. Also the values for the tested algorithms are greater than 30 dB which show that these systems have good quality.

Table II indicates results of applying PSNR on the color images. As the results show there is also improvement in the quality of stego-images using proposed algorithm in comparison with the DCT and 4th bit method. Noted that all the values are greater than 30dB which show that the proposed system is acceptable.

TABLE I: PSNR RESULTS OF 25 SAMPLE GRAYSCALE STEGO-IMAGES AFTER EMBEDDING 40 BYTES

Image Type	AVERAGE PSNR	
	DCT & 4TH BIT	GA-BASED DCT & 4TH BIT
Building	64.4870	67.3875
Flower	55.7139	61.7018
Mountain	64.6570	67.7601
People	56.9060	63.9616
Tree	54.8445	62.1182

TABLE II: PSNR RESULTS OF 25 SAMPLE COLOR STEGO-IMAGES AFTER EMBEDDING 40 BYTES

Image Type	Average PSNR	
	DCT & 4^{th} bit	GA-based DCT & 4^{th} bit
Building	66.0981	73.9122
Flower	68.6862	70.7069
Mountain	66.1770	75.7129
People	67.5921	71.4356
Tree	67.9701	72.5088

TABLE III: RESULTS OF CHI-SQUARE ATTACK FOR GRAYSCALE STEGO-IMAGES

Image Type	Chi-square Test Probability	
	JSTEG	GA-based DCT & 4^{th} bit
Building	0.4634	0
Flower	0.7408	0
Mountain	0.9082	0.211×10^{-10}
People	0.6424	0
Tree	0.7462	0.318×10^{-13}

Fig. 2 also shows the experimental results for a grayscale "lena.jpg" image, before and after embedding 500 bytes information and their histograms. In this figure (a) shows the original image and its histogram; (b) and (c) indicate embedding of 500 Bytes using DCT and 4^{th} bit, and the proposed methods respectively.

As Fig. 2 illustrates there is more changes in the histogram of stego-image applying DCT and 4^{th} bit algorithm in comparison with the histogram of the stego-image created by the proposed method. PSNR value also verifies this result.

B. Robustness Evaluation

As mentioned previously, besides imperceptibility and capacity the steganographic systems have another goal that is robustness. Some steganaylsis techniques have developed to determine the existence of messages in cover objects. Chi-square attack is used for evaluating our proposed system and comparing it with another steganographic algorithm called JSTEG which was broken by this attack [10].

The attack is applied on 25 sample grayscale images and the maximum result for every category is presented in table III for embedded message of 1000 bytes. As table III shows the attack can detect that there is message in the stego-image created by JSTEG and the maximum probability is for mountain images with value of 0.9082 (90.82%), but there is no detection for the proposed algorithm.

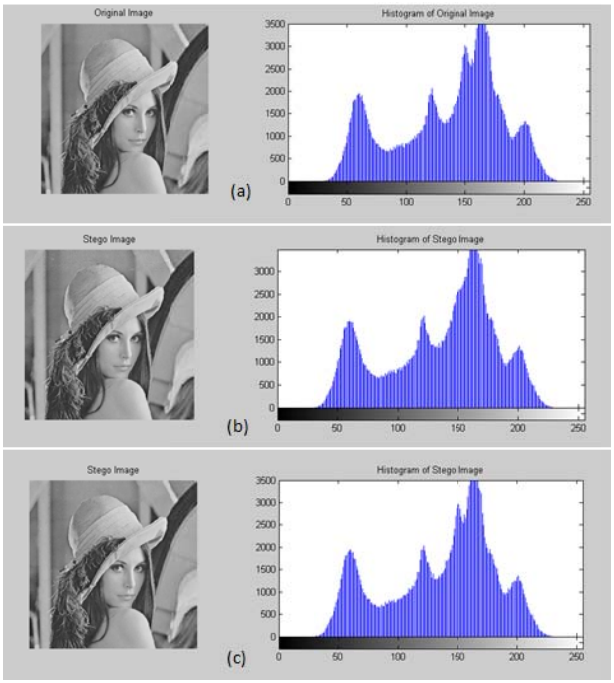

Fig. 2. (a) Lena image before embedding, (b)Lena image after embedding 500 bytes using DCT and 4th bit algorithm (PSNR=40.82dB), (c) Lena image after embedding 500 bytes using our proposed algorithm (PSNR=46.38dB)

VI. CONCLUSION

In this paper a robust genetic based image steganography method was proposed. The message is embedded in 4^{th} bit of DCT coefficients of an image. The idea is derived from the fact that embedding message in more significant bits of the image makes it more resistant against different attacks.

However, as embedding message in these bits causes higher differences between the original image and the steganogram, so some modification must be done to make these differences as least as possible. Therefore an optimization algorithm called genetic was used to optimize the steganogram.

This method designed and coded, then different tests performed to evaluate different aspects of the proposed scheme. As the experimental results show there is improvement in quality and undetectability of the proposed system.

In addition, DWT is another frequency domain transformation technique used in image steganography. Therefore the proposed technique can be applied in DWT instead of DCT to see whether there is an improvement in different aspects of the system. This assumption needs more investigation and research to be done. So the future work will focus on this assumption.

ACKNOWLEDGMENT

We offer our regards and blessings to all of those who supported and guided us in any respect during the completion of this project.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, Mar. 2010.

[2] C. Stanley, "Pairs of values and the chi-squared attack," Master thesis, Dept. Mathematics, Iowa State University, 2005.

[3] S. M. Thampi, "Information hiding techniques: a tutorial review," *ISTE-STTP on Network Security and Cryptography*, LBS College of Engineering, Kasaragod, 2004.

[4] K. B. Raja, *et al*., "Genetic algorithm based steganography using wavelets," *Information Systems Security*, Springer-Verlag, pp. 51-63, 2007.

[5] N .F. Johnson and S. C. Katzenbeisser, "A survey of steganographic techniques," in *Proc. of information hiding techniques for steganography and digital watermarking*, 2000, pp. 43-78.

[6] A. Khayam, *The Discrete Cosine Transform (DCT): theory and application*, Michigan State University. Mar. 2003.

[7] S. Mitra and T. Acharya, *Data Mining: Multimedia, Soft Computing, and Bioinformatics*, New York: Wiley, 2003.

[8] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Trans. Image Processing*, vol. 12, pp. 221-229, Apr. 2003.

[9] N. Kafri1 and H. Y. Suleiman, "Bit-4 of frequency domain-DCT steganography technique," in *Proc. of Networked Digital Technologies*, IEEE, 2009, pp. 286-291.

[10] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," *Information Hiding*, vol. 1768/2000, Springer-Verlag, pp. 61−76, 2000.

[11] N. Provos, "Defending against statistical steganalysis," in *Proc. of USENIX Security Symposium*, 2001, pp. 24-36.

[12] J. Rodrigues, J. Rios, and W. Puech, "SSB-4 system of steganography using bit 4," *in Proc. of International Workshop on Image Analysis for Multimedia (WIAMIS 2004)*, 2004.

[13] C. P. Wah, "Digital video watermarking techniques for secure multimedia creation and delivery," Master thesis, Chinese University, Hong Kong, July 2004.

[14] A. Milani Fard, M. R. T. Akbarzadeh, and F. Varasteh, "A new genetic algorithm approach for secure JPEG steganography," in *Proc. of Engineering of Intelligent Systems*, IEEE, 2006, pp. 1-6.

[15] P. Sallee. (2003). Matlab JPEG toolbox. [Online]. Available: http://www.philsallee.com/jpegtbx/index.html.

Zahra Moghaddasi was born in Iran. She graduated with B.Sc. Computer Engineering (Software Engineering) from Amir Kabir University of Technology in Tehran, Iran in 2007, and M.Sc. Computer Science (Information Security) from University Technology Malaysia in Kuala Lumpur, Malaysia in 2011. She did several software projects and developed steganography software. Her current areas of interest and research are image processing, steganography, digital computer forensics, and network security

Azizah Abdul Manaf is a Professor of Image Processing and Pattern Recognition from Universiti Teknologi Malaysia (UTM). She graduated with B. Eng. (Electrical-Communication & Control) in 1980, M.Sc. Computer Science (1985) and PhD (Image Processing) in 1995 from UTM. She has co-authored books, written numerous articles in journals and presented an extensive amount of research papers at national and international conferences on her area of expertise. She has also held management positions at the University and Faculty level such as Head of Department, Deputy Dean, Deputy Director and Academic Director pertaining to academic planning and development as well as coordinating training on teaching and learning methodologies for students and lecturers at the University. Her current areas of interest and research are image processing and pattern recognition, watermarking, steganography and digital computer forensics.