# A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain

M. Soleimanpour*, S. Talebi* and H. Azadi-Motlagh*

**Abstract:** This paper devotes itself to the study of secret message delivery using cover image and introduces a novel steganographic technique based on genetic algorithm to find a near-optimum structure for the pair-wise Least-Significant-Bit (LSB) matching scheme. A survey of the related literatures shows that the LSB matching method developed by Mielikainen, employs a binary function to reduce the number of changes of LSB values. His method verifiably reduces the probability of detection and also improves the visual quality of stego images. However, his method still has room for improvement. In this paper, a dual-state scoring model, structured upon genetic algorithm is presented which assesses the performance of different orders for LSB matching and searches for a near-optimum solution among all the permutation orders. Experimental results confirm the superiority of the new approach compared to the Mielikainen's pair-wise LSB matching scheme in terms of distortion.

**Keywords:** Genetic Algorithm, LSB Matching, Steganograghy.

## 1 Introduction

Steganography is derived from the Greek words *steganos* meaning "covered or protected" and *graphei* meaning "writing". As defined by Cachin [1], steganography is the art and science of communicating in a way that the presence of a secret message apart from the identity of sender and intended recipient cannot be detected, in other words, it is a form of security through obscurity. Techniques to hide information have been in use for hundreds of years, but with the increasing use of file transfers in an electronic format, Steganography and watermarking are spearheading the enormous growth of advanced algorithms to hide important (secret) information in an undetectable and/or irremovable (secure) way in audio and video fields and they are, therefore, the main focus in any information concealment activity [2-4].

Images that are used for inserting and hiding secure data are called 'cover images' and the image in which secret bits are inserted is known as 'stego image'.

Steganography platforms can be divided into two main categories, namely; spatial domain and transform domain. In the transform domain, Discrete Cosin Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) are the most common examples [5], being the preferred schemes due to lower computational complexities and higher resistances against compression which are key advantages.

In the DCT based steganography, the two key points to consider are; a- selection of DCT coefficients, i.e. the choice of higher frequencies makes presence of the image unrecognizable, and, b- magnitude of changes applied to DCT coefficients in order to insert signature in the image. Changes of the coefficients have an effect on the secrecy of signature and can even distort the image a great deal.

The first attempt in spatial domain is LSB substitution. LSB substitution steganography is a popular and simple technique that hides message bits in LSB of image pixels. It should be mentioned that the Mielikainen's method reduces the probability of detection but simultaneously it decreases the visual quality of images. Therefore finding the best matching order based on the Mielikainen's method principle in order to reduce the distortion of the stego images by applying the heuristic search algorithms such as Genetic algorithm [6], Particle Swarm Optimization (PSO) [7] for JPEG images, Immune Programming Algorithm (IP) [8] are proposed recently. In our proposed method, Genetic Algorithm (GA) is employed to inspect a score matrix in order to find the best LSB matching order. This method not only is an improvement on the Mielikainen's method but also speeds up the algorithm and decreases probability of detection.

The rest of the paper is organized as follows:

Iranian Journal of Electrical & Electronic Engineering, 2013.
Paper first received 28 Nov. 2012 and in revised form 12 Mar. 2013.
* The Authors are with the Department of Electrical Engineering, Bahonar Univesity of Kerman, Kerman, Iran.
E-mails: mohadese.soleimanpour@yahoo.com and Siamak.Talebi@uk.ac.ir.

In Section 2, an overview of other steganography methods is given. Section 3 details our proposed method. In Section 4, the experimental results are shown and discussed. Finally, the conclusions are presented in Section 5.

## 2 Review of Steganography Methods

Steganography, as a core of information hiding, is the art of embedding a secret message imperceptibly within the cover image (e.g, digital images in this paper). In steganography techniques, many different cover file formats can be used but because of wide spread application of digital images on the internet, they have become the most popular format [9].

Methods of image steganography can be divided into two groups: Transform Domain techniques and Spatial Domain methods [2]. In the Transform Domain technique, images are first transformed and then the message is embedded in the cover image [10].

The Transform Domain steganography methods hide messages in more significant areas of the cover image, and this requires the cover image to split into high, middle and low frequency components.

Since most of the signal energy is concentrated in the lower frequencies, which is very important in visibility, therefore, secret data is embedded in the higher frequencies in order to avoid image distortion.

Most Transform Domain methods are independent of the image format and as a result the embedded message may survive conversion between lossy and lossless compression [11].

Good security and robustness against statistical attacks and image manipulation are the most important advantages of these methods. However, high computational complexity is the main concerns here.

In the Spatial Domain methods, messages are embedded in the intensity of the pixels directly.

One of the popular methods is to embed secret messages into the cover image by directly manipulating the least-significant bit (LSB) plane [12, 13]. In LSB substitution, LSB bits of cover image is replaced with secret bits. One significant drawback of this method is that the secret message can be detected very easily [14]. Although it is not the best steganographic method, it is worth studying it because of its simplicity.

Because of high probability of detection in LSB substitution, a new method based on embedding the information into the cover image has been developed which is called LSB matching [12].

In the LSB matching method, first a matching process between the secret message and the cover image is performed and then embedding takes place based on the maximum similarity [15].

A survey of published literature shows that LSB matching is successful as a steganographic method prticularly for gray scale images at embedding rates [16-21]. However, the main disadvantage of this approach is that traditional detectors [22, 12] are not effective (enough) against LSB replacement for LSB matching steganography.

The performance of the LSB matching technique has been further improved by the Mielikainen's method [23] in which the LSBs of the cover image are not just simply replaced with LSB of the secret message. In the Mielikaien's method, if the message bit does not match the LSB of the cover image then one is randomly either added or subtracted from the value of the cover pixel.

### 2.1 A Brief Review of the Mielikainen's Method

In this method, firstly, matrix of cover image $H$ and secret message $S$ are converted into streams of $H_0$ and $S_0$, respectively, as follows:

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} & \cdots & h_{1c} \\ h_{21} & h_{22} & h_{23} & \cdots & h_{2c} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{rc} & h_{r2} & h_{r3} & \cdots & h_{rc} \end{bmatrix}$$

$$\begin{bmatrix} h_{11} h_{12} h_{13} \cdots h_{1c} h_{21} h_{22} h_{23} \cdots h_{2c} \cdots h_{r1} h_{r2} h_{r3} \cdots h_{rc} \end{bmatrix}$$

then, each two consecutive elements in the streams of $H_0$ and $S_0$ are selected. Assume that the two cover pixels are $x_i$ and $x_{i+1}$, and also that the two secret bits to be hidden are $m_i$ and $m_{i+1}$.

The method is performed as follows: first the value of secret bit $m_i$ is compared with the LSB of the first cover pixel $x_i$ If they are equal ($m_i$=$LSB$($x_i$)), then the first cover pixel is kept unchanged, $y_i = x_i$, otherwise, the second cover pixel is kept, $y_{i+1} = x_{i+1}$. When $y_i = x_i$, $m_{i+1}$ is compared with $f(x_i, x_{i+1})$ where $f(x_i, x_{i+1})$ is defined as follows:

$$f(x_i, x_{i+1}) = LSB\left(\left\lfloor \frac{x_i}{2} \right\rfloor + x_{i+1}\right) \quad (1)$$

If they are equal, then $y_{i+1} = x_{i+1}$, otherwise, the second pixel $y_{i+1}$ is calculated by randomly incrementing/decrementing the second cover pixel $x_{i+1}$. If $m_i$ is not equal to $LSB(x_i)$, then $y_{i+1} = x_{i+1}$. If $m_{i+1} = f(x_i - 1, x_{i+1})$, then the value of $y_i = x_i - 1$, otherwise, $y_i = x_i + 1$. The Mielikainen's method is flowcharted in Fig. 1.

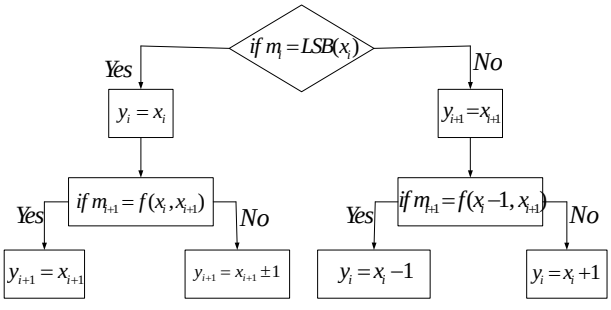



**Fig. 1** Flowchart of Meilkainen's method

Although the Mielikainen's method reduces the probability of detection but it may also distort stego images. The matching order of the secret data and cover image can be further adjusted to reduce the distortion of the stego images by applying the heuristic search algorithms such as Particle Swarm Optimization (PSO) [7] for JPEG images, Immune Programming Algorithm (IP) [8] or Genetic Algorithm Optimization priority adjustment process. In the next section the proposed method is described in greater detail.

## 3 Proposed Method

From the flowchart in Fig. 1, it can be stated that the best matching with fewer changes of the cover image is achieved when $m_i = LSB(x_i)$ and $m_{i+1} = f(x_i, x_{i+1})$, which means values of stego pixel $y_i$ and $y_{i+1}$ and cover pixel $x_i$ and $x_{i+1}$ are equal, respectively, and as a result the difference between stego image and the cover image is minimal.

In our proposed method, a dual state-scoring, designated by $T_i$ is used that operates as follows:

1. When two cover image pixels are similar to stego image pixels, score is $T_1$.
2. When one of the stego image pixels changes relative to cover image, score is $T_2$.

In order to show that keeping the cover pixel values unchanged is superior to letting them change, they must be assigned based on fewer changes of cover image. Now, in order to achieve this aim, $T_1$ is assumed to be greater than $T_2$, $(T_1 > T_2)$. In other words, pixel embedding without the requirement for LSB change is more desirable than embedding where change of LSB is required.

### 3.1 Score Matrix

In order to evaluate the performance of different matching order of secret image and cover image, a matrix called score matrix $M$ is calculated.

Assume that S and H are the matrix of secret data and cover image, respectively. Firstly, by scanning S and H left-to-right and top-to-bottom, these matrices get converted into streams of $H_0$ and $S_0$, respectively.

Then, for each two sequential pixels in the stream the value of $T$ is first evaluated and then based on these calculations score matrix $M_{L_s * L_h}$ is constructed as follows:

$$M_{L_s * L_h} = \left\{ \begin{matrix} m(i,j) \,|\, m(i,j) \in \{T_1, T_2\} \\ 1 \le i \le L_s \quad , \quad 1 \le j \le L_h \end{matrix} \right\} \tag{2}$$

where $m(i, j)$ is the $i$-th row and the $j$-th column element of this matrix $M$, $L_s$ is the length of secret stream groups and $L_h$ is the length of cover stream groups. In order to find the best matching order we need to choose $L_s$ element in different row and columns from the matrix $M$. It should be mentioned that only one element from each row and column must be selected [8].

Accordingly, an adjustment list is evaluated from these selected $L_s$ elements, namely; $J = [j_1, j_2, ..., j_k, ..., j_{L_h}]$, where index k indicates the $k$-th column of $M$ and the value of $j_k$ refers to the $j_k$-th element of $k$-th column.

If $L_h > L_s$, it means that the cover stream is greater than the secret stream, then $j_k$ will be set to -1, declaring that the $k$-th group of the cover stream will not embed any secret information.

If $L_h = L_s$, it means that all the groups of the cover stream will embed their corresponding secret data and the adjustment list $J$ does not have any -1 element.

It should be noted that many adjustment lists can be built by taking different elements and eventually the one with the highest score will be the best matching structure. The Heuristic search algorithm can be used to obtain the best adjustment list.

In this paper a genetic algorithm is exploited to find the optimal adjustment. For simplicity, the normalized total score of $J$ is introduced as follows:

$$f(J) = \frac{1}{f^m} \sum m(i,j)\,|_J \tag{3}$$

$$f^m = L_s . T_1 \tag{4}$$

where $f^m$ is the maximum value for the adjustment list.

### 3.2 Genetic Algorithm Strategy

Over the past several decades, population-based optimization search techniques, such as evolutionary algorithm [24], ant colony optimization [25], particle swarm optimization [26], gravitational search algorithm [27, 28], artificial bee colony [29], etc. [30, 31], have been applied to solve global optimization problems. Natural evolution or phenomena have been the motivation behind development of these algorithms.

Population-based algorithms offer a collection of potential solutions for a given problem where the operators act on population and produce collections of new solutions. This process is repeated until the stopping criteria are met.

The population-based optimization algorithms often perform well to approximate solutions to a wide range of problems [32-35]. GA is a heuristic search that mimics the process of natural evolution. This heuristic search is routinely adopted to generate useful solutions to optimization and search problems [36]. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as mutation, selection and crossover.

Crossover and mutation are the processes for exploration and exploitation of the population. Selection is an act of picking out the best agent from the population according to the GA principles.

In the proposed method, in order to perform LSB matching, we use a GA strategy to find a near optimal adjustment list.

#### 3.2.1 Initialization

At first, many individual solutions are randomly generated to form an initial population. As said before, we need to find the optimal adjustment list J in order to perform LSB matching so that the distortion of the stego image can be minimized. In the Genetic algorithm, the population represents the solution. Thus, for initialization, an initial population, P of N chromosome, $P_i$ $i = 1, \ldots, N$ , is generated randomly.

#### 3.2.2 Fitness Evaluation

The fitness of each individual in that population is evaluated based on fitness function.

#### 3.2.3 Parent Selection

After fitness evaluation, parents are chosen based on their fitness. During each iteration, a percentage of the existing population is selected (which is called parents) to create a new population. Parents are selected through a fitness-based process, where fitter solutions (as measured by a fitness function) are typically more likely to be selected. The selection procedure picks out two parent chromosomes, based on their fitness values, which are then used by the crossover and mutation operators (described below) to produce two offspring for the new population. In this paper, roulette wheel is used for the selection procedure. In roulette wheel selection, individuals are given a probability of being selected that is directly proportionate to their fitness. Afterward, two individuals are chosen randomly, based on these probabilities, to produce new population.

#### 3.2.4 Crossover

Crossover is one of the basic operators of GA which determine (define) the performance of GA. There are many ways for carrying out a crossover. Type and implementation of operators depend on the encoding as well as on the problem under study.

According to our experiment, one point crossover is the best choice in our case. In order to achieve this aim, a pair of chromosomes which has been selected in the selection step is used by crossover. At first, a random number between 0 and 1 is generated and compared to a parameter called the probability of crossover, $P_c$. If the random number is larger than $P_c$, then two parents are chosen randomly from the population P, and the left and right parts of these two agents are exchanged. On the other hand, if the random number is not larger than $P_c$, then crossover will not happen. The crossover probability can be changed from 0.0 to 1.0. Our empirical studies have shown that better results are achieved by a crossover probability of 0.7, which implies that the probability of a selected chromosome surviving to the next iteration unchanged (apart from any changes arising from mutation) ranges from 0.3.

#### 3.2.5 Mutation

Mutation like crossover is one of the basic operators of GA. Decision on the best method to implement mutation is again affected by the type of encoding as well as on the kind of problem at hand. In the mutation procedure, a random number between 0 and 1 is generated and compared to a parameter called probability of mutation, $P_m$. If the random number is larger than $P_m$, then a gene is selected randomly from the current population, P, and the genes on this population are changed, e.g. 0 becomes 1 and vice versa. Then this mutated gene will be placed back into population of the current generation. If the random number is less than $P_m$, no operation will be carried out.

In order to do mutation operator, each bit in each chromosome is checked for possible mutation by generating a random number between zero and one and if this number is less than or equal to the given mutation probability, e.g. 0.001, then the bit value is changed.

#### 3.2.6 Generating a New Population

After the last three steps, new population is generated.

#### 3.2.7 Stopping Criteria

The algorithm, previously described, carries out the steps one by one in sequence and when they have been performed it is said that one generation has passed. At the end of each generation Genetic algorithm checks stop criteria. Because of the nature of Genetic algorithms, most of the times it is not clear when the algorithm should stop, so the criterion is usually based on statistical information such as number of generation, fitness value of the best chromosome or average fitness value of chromosomes in the population, duration of evolution process and so on.

The flowchart of genetic algorithm is shown in Fig. 2. The basic steps for GA are described as shown in Fig. 2.

### 3.3 Improved Version of Genetic Algorithm

In order to match genetic algorithm by proposed problem a new kind of cross over and mutation are proposed. As it explained before, the proposed problem is finding a near optimal solution in a discrete search space. In this section, in order to simplify the problem, the problem is solved when size of secret image and cover image are equal. By this assumption, each chromosome in population is a disorder vector of number 1 to $L_h$.

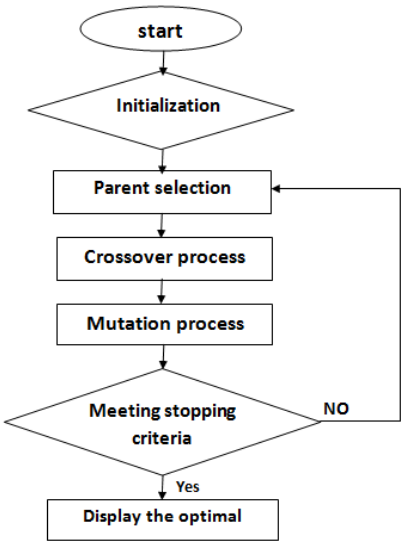



**Fig. 2** Flowchart of Genetic Algorithm

The most important issue in this problem is that testing every possibility for disordering a $L_h$ number would be $L_h$ math additions. As an example, a $L_h = 30$ number would have to measure the total distance of be $2.65 \times 1032$ different disorder vector. Assuming a trillion additions per second, this would take 252, 333, 390, 232, 297 years. Adding one more number would cause the time to increase by a factor of 31. Obviously, this is an impossible solution. This is the same problem, when we want to have a complete search in the steganography matching problem.

As it explained before, each chromosome is assumed as a disorder vector of number 1 to $L_h$. In the crossover step, after choosing two parents in order to create the children, every item in the parent's sequence after the crossover point is swapped. The difficulty in this problem is that every element can only be used once in a vector. In order to solve this issue, every element after the crossover point is checked. If the checked element is already existed in the child, a non-selected element is selected randomly.

The mutation step is also changed in this algorithm. As we cannot change the gene's bits as the usual traditional mutation does. Instead we must swap the order of just two elements in each chromosome.

By changing these two steps, the improved version of genetic algorithm is in an exact harmony by the proposed problem.

The pseudo code for constructing a stegano image is explained In the following steps:

a. Change the gray scale secret image into binary image
b. Evaluate the score matrix in accordance with (in relation to) the Mielikainen's method.
c. Define the fitness function in order to calculate the adjustment list value.
d. Find the best adjustment list by using the genetic algorithm strategy.
e. Embed the secret data into the cover image in accordance with the adjustment list.
f. End.

### 3.4 Data Extraction

As said in [8], during the data extraction process knowing the adjustment list J in order to extract the data for receiver is essential. The steps in the algorithm can be summarized as follows:

**Step 1.** The stego stream $S_{t_0}$ will be arranged by scanning the stego image $S_t$ from top-to-bottom and from left-to-right.

**Step 2.** Each consecutive two elements of the stream $S_{t_0}$ is considered as a group. For the $i$ th group of the stream the $i$ th position of $J$ has been checked. If the $i$ th value is not -1, the value of second secret bit $m_{i+1}$ is calculated by using Eq. (1).

**Step 3.** If $m_{i+1} = LSB(y_i)$, the first secret bit $m_i$ is $m_{i+1}$. If $m_{i+1}$ is not equal to $LSB(y_i)$, then $m_i$ is calculated from $m_i = f(y_i, y_{i+1} \pm 1)$.

**Step 4.** When the entire secret bit groups have been extracted, the inverse manipulation of step 1 is executed in order to arrange the secret image.

## 4 Experimental Result

To validate the performance of the proposed method, several experimental results are presented and discussed in this section. In our experimental assessments all images are 256 gray levels of size 512 × 512. We take the images Jet, Cameraman, Baboon, House, Pepper and Man [8], separately shown in Figs. 3-a, b, c, d, e and f, as cover images. The image of Coins (Fig. 3-g) is taken as secret information. The size of the original secret images is 256 × 256 with 256 gray levels. In the proposed method the secret image needs to be a binary image, so as to allow the threshold value to be used to convert the gray scale image into a binary image. In this paper, an automatic thresholding is utilized to produce a binary image.

Table 1 displays PSNR values derived from the proposed method versus those obtained from the Mielikainen's method. From the table, it is evident that the proposed method achieves higher PSNR values for different stego images compared with the Mielikainen's and as a result the visual quality of images processed by our scheme are better.

As mentioned before, when the difference between the LSB value of the stego image and cover image rises the visual quality of the stego image falls. Table 2 compares percentages of LSB position changes for different stego images. As can be seen from this table, LSB position changes less frequently for Jet, Cameraman, Baboon, House, Pepper and Man images as a result of employing the proposed method.

a. Cover image 1

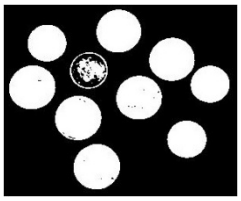
b. Cover image 2

c. Cover image 3

d. Cover image 4

e. Cover image 5

f. Cover image 6



g. Secret image

**Fig. 3** Images in our experiments

**Table 1** PSNR value comparison

| | **Mielikainen's method** | **Proposed method** |
|---|---|---|
| **Jet** | 52.36933 | 53.15158 |
| **Cameraman** | 52.35057 | 53.18642 |
| **Baboon** | 52.37549 | 53.31759 |
| **House** | 52.43724 | 53.25734 |
| **Peppers** | 52.42461 | 53.22971 |
| **Man** | 52.40562 | 53.23653 |

**Table 2** Comparison of LSB changes (in percentages)

| | **Mielikainen's method** | **Proposed method** |
|---|---|---|
| **Jet** | 15.27 | 11.46 |
| **Cameraman** | 15.42 | 11.27 |
| **Baboon** | 15.18 | 10.71 |
| **House** | 14.66 | 11.03 |
| **Peppers** | 15.19 | 11.19 |
| **Man** | 15.18 | 11.14 |

From the above two tables it can be argued that since the proposed method achieves higher PSNR values and reduces the number of changes of LSB position, visual quality of the stego images improve noticeably compared with the original pair-wise LSB matching steganography.

a b

**Fig. 4** a) Image of Cameraman before embedding secret data and b) Image of Cameraman after embedding secret data

a b

**Fig. 5** a) Image of Peppers before embedding secret data and b) Image of Peppers after embedding secret data

### 4.1 Invisibility Test

Fig. 3 shows the cover image and secret data which (in this case) is the image of a coin. The stego images are shown in Figs. 4-b and 5-b which were generated after data was embedded into the LSB planes using the proposed method. It can be said that the visual quality of the stego images is not degraded much significantly. Similar tests were also performed on the other images, yielding the same results.

### 4.2 The Probability of Detection Test

A review of the related literature shows that a variety of detectors have been introduced by Westfeld [21], Harmsen [17] and Liu et al. [19, 20]. In our experiments, firstly, calibrated HCF COM is used and then the calibrated adjacency HCF COM is utilized to evaluate the performance of the LSB matching, the Mielikainen's and the proposed methods.

In Fig. 6, receiver operating characteristic (ROC) curves using the calibrated HCF COM for message detection has been sketched. The above plot displays variation of detection probabilities and false positive for different methods as the detection threshold is adjusted. It is clearly seen that the proposed method results in an improved detection probability.

As shown in Fig. 7, it can be seen that our proposed solution reduces the probability of detection for the HCF COM detectors compared to both the LSB matching and the Mielikainen's schemes. In order to focus on a region of interest the *x*-axis has been scaled.

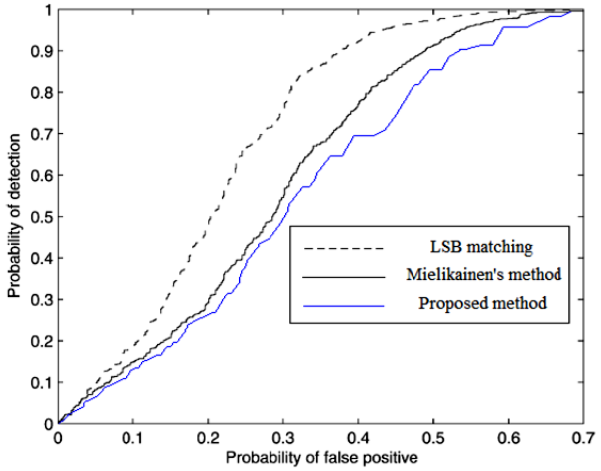



**Fig. 6** ROC curves for calibrated HCF COM

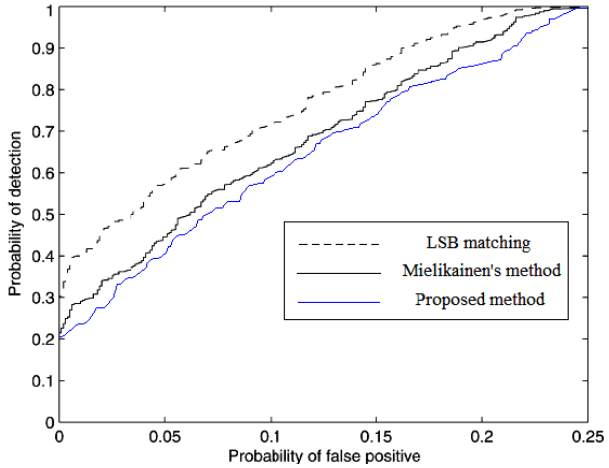



**Fig. 7** ROC curves for calibrated adjacency HCF COM

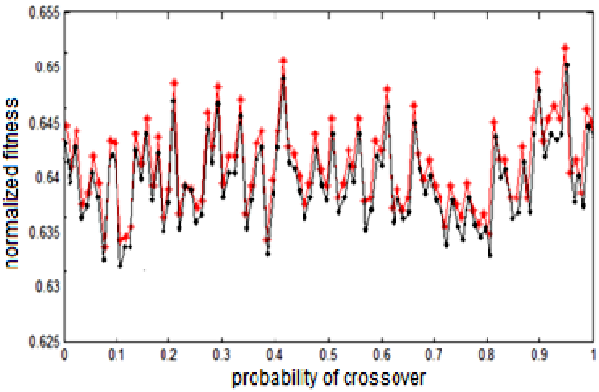



**Fig. 8** Fitness evalution for different values of crossover probability

In Fig. 8, the sensitivity of the proposed method against probability of crossover is illustrated. It was seen in Fig. 8 that when the value of $P_c$ is close to 0.427 the normalized value of fitness is maximized.

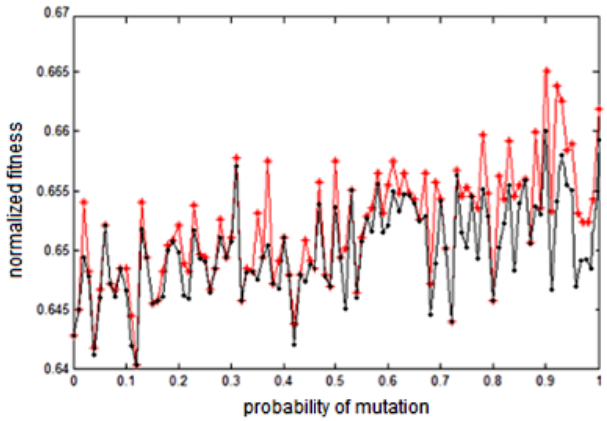



**Fig. 9** Fitness evaluation for different values of mutation probability

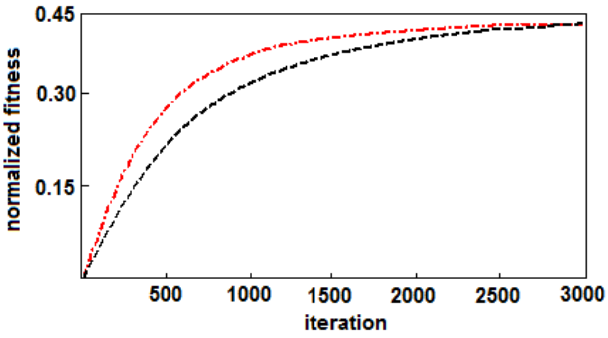



**Fig. 10** Convergence rate of proposed method

Similarly, in Fig. 9, sensitivity of the proposed method versus probability of mutation is plotted. In this case, the best value of $P_m$ is when it is close to 0.901 which may seem a large value for mutation process but it was obtained because of multimodality of fitness function. On the other hand, for this fitness function the probability of trapping in local optima are high. Therefore, in order to increase the exploration ability of algorithm, the probability of mutation should be increased.

The convergence rate of the proposed method based on generation is plotted in Fig. 10. Here, the red curve shows the best fitness value so far and the black curve indicates the average fitness value. As can be seen, by increasing the generations improved score values can be obtained. Fig. 10 also illustrates that all agents converge in the last 20 percent of generation.

### 4.3 Complexity Comparison

When the complexity of the proposed method is compared against that of the Mielikainen's, it is seen that our approach is more complex. It should be noted, however, that the Mielikainen's model suffers from two undesirable effects, namely; it decreases the visual quality of the image and simultaneously increases the probability of detection which already has been proved. It can be concluded that the proposed method achieves

as a result of an extra complexity but it has more robust and higher visual quality, therefore it is an acceptable procedure which are advantages desired in steganography.

## 5 Conclusion

This paper presented a new LSB matching method based on Genetic algorithms. The proposed solution evaluated different LSB matching structures and devised a score-matrix system. The main advantages offered by this innovative scheme are higher PSNR values of stego images and a reduction in the number of changes of LSB position resulting in an improved visual quality of stego images. An examination of the simulation results also confirmed that the proposed technique outperforms many of the popular techniques put forward by Mielikainen and others. One drawback of this model as was revealed by experiments is that for some stego images the duration for calculating the score matrix is comparatively long. Authors are currently exploring new approaches to overcome this minor hitch.

## References


[1] Cachin C., "An Information-Theoretic Model for Steganography", *Proceedings of 2ndWorkshop on Information Hiding, MIT Laboratory for Computer Science*, pp. 306-318, 1998.

[2] Silman J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001.

[3] Sachnev V., Kim H. J., Nam J., Suresh S. and Shi Y. Q., "Reversibel watermarking algorithm using sorting and prediction", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 19, No. 7, pp. 989-999, 2009.

[4] Mohammadi S., Talebi S. and Hakimi A., "Two Novel Chaos-Based Algorithms for Image and Video watermarking", *Iranian Journal of Electrical & Electronic Engineering*, Vol. 8, No. 2, pp. 97-107, 2012.

[5] Wang Y. and Moulin P., "Steganalysis of block-DCT image steganography", *IEEE workshop on Statistical Signal Processing, IEEE Computer Society Press*, Los Alamitos, pp. 339-342, 2003.

[6] Liu G., Zhang Z. and Dai Y., "GA-based LSB-matching steganography to hold second-order statistics", *Proceedings of MINES'09 Los Alamitos IEEE Computer Society*, pp. 510-513, 2009.

[7] Liu X. X. and Wang J. J., "A steganographic method based upon JPEG and swarm optimization algorithm", *Information Science*, Vol. 177, No. 15, pp. 3099-3109, 2007.

[8] Xu H., Wang J. and Kim H. J., "Near-optimal solution to pair-wise LSB matching via an immune programming strategy", *Information Sciences*, pp. 1201-1217, 2010.

[9] Fabien A. P., Ross J. Anderson and Markus G., "Information Hiding - A Survey", *Proceedings of the IEEE, special issue on Protection of Multimedia Content*, pp. 1062-1078, 1999.

[10] Lee Y. K. and Chen L. H., "High capacity image steganographic model", *IEE Proceedings of Visual Image Signal Processing*, Vol. 147, No. 3, pp. 288-294, 2000.

[11] Shi Y. Q. and Sun H., *Image and Video Compression for Multimedia Engineering*, CRC Press, Boca Raton London New York Washing, D.C., 2001.

[12] Ker A., "Improved detection of LSB steganography in grayscale image", *Lecture Notes in Computer Science*, pp. 97-115, 2005.

[13] Mahdavi M., Samavi Sh., Zaker N. and Modarres-Hashemi M., "Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram", *Iranian Journal of Electrical & Electronic Engineering*, Vol. 4, No. 3, pp. 59-70, 2008.

[14] Chan C. K. and Chan L. M., "Hiding data in image by simple LSB substitution", *Pattern Recognition*, Vol. 37, pp. 469-467, 2004.

[15] Chang C. C., Hsiao J. Y. and Chan C. S., "Finding optimal least-signification-bit substitution in image hiding by dynamic programming strategy", *Pattern Recognition*, Vol. 36, pp. 1583-1595, 2003.

[16] Fridrich J., Soukal D. and Goljan M., "Maximum likelihood estimation of length of secret message embedding using y dynamic programming strategy", *Proceedings of SPIE Electronic Imaging 5681*, 2005.

[17] Harmsen J. and Pearlman W., "Steganalysis of additive-noise modelable information hiding", *Proceedings of the SPIE Security Watermarking Multimedia Contents 5020*, 2003.

[18] Ker A., "Steganalysis of LSB matching in grayscale images", *IEEE Signal Processing Letters*, Vol. 12, No. 6, pp. 441-444, 2005.

[19] Liu Q. Z., Sung A. H., Xu J. Y. and Ribeiro B. M., "Image complexity and feature extraction for steganalysis of LSB matching steganography", *The 18th International Conference on Pattern Recognition*, Vol. 2, pp. 267-270, 2006.

[20] Liu Q. Z., Sung A. H., Chen Z. X. and Xu J. Y., "Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images", *Pattern Recognition*, Vol. 41, No. 1, pp. 56-66, 2008.

[21] Westfeld A., "Detecting low embedding rates", *Lecture Notes in Computer Science 2578*, pp. 324-339, 2002.

[22] Fridrich J., Goljan M. and Soukal D., "Higher-order statistical steganalysis of palette images", *Proceedings of the SPIE Security Watermarking Multimedia Contents 5020*, 2003.

[23] Mielikainen J., "LSB matching revisited", *IEEE Sigal Processing Letters*, Vol. 13, No. 5, pp. 285-287, 2006.
[24] Tu Z. and Lu Y., "A robust stochastic genetic algorithm (SGA) for global numerical optimization", *IEEE Transactions on Evolutionary Computation*, Vol. 8, pp. 456-470, 2004.
[25] Baojiang Z. and Shiyong L., "Ant colony optimization algorithm and its application to neuro-fuzzy controller design", *Journal of Systems Engineering and Electronics*, Vol. 18, pp. 603-610, 2007.
[26] Hsieh S. T., Sun T. Y., Lin C. L. and Liu C. C., "Effective learning rate adjustment of blind source separation based on an improved particle swarm optimizer", *IEEE Transactions on Evolutionary Computation*, Vol. 12, No. 2, pp. 242-251, 2008.
[27] Rashedi E., Nezamabadi-pour H. and Saryazdi S., "GSA: a gravitational search algorithm", *Information Science*, Vol. 179, No. 13, pp. 2232-2248, 2009.
[28] Moghadam M. S., Nezamabadi-Pour H. and Farsangi M. M., "A Quantum Behaved Gravitational Search Algorithm", *Intelligent Information Management*, Vol. 4, No. 6, pp. 390-395, 2012.
[29] B. Akay and D. Karaboga, "A modified artificial bee colony algorithm for real-parameter optimization", *Information Sciences*, Vol. 192, pp. 120-142, 2010.
[30] Reynolds R. G., "An introduction to cultural algorithms". *Proceedings of the third annual conference on evolutionary programming*, pp. 131-139, 1994.
[31] Soleimanpour-Moghadam M. and Nezamabadi-Pour H., "An improved quantum behaved gravitational search algorithm", *20th Iranian Conference on Electrical Engineering, Iran*, 2012.
[32] Sofge D., Jong K. De and Schultz A., "A blended population approach to cooperative coevolution for decomposition of complex problems", *in: Proceedings of the 2002 Congress on Evolutionary Computation*, Vol. 1, pp. 413-418, 2002.
[33] Qiana B., Wanga L., Huanga D. X., Wangc W.L. and Wang X., "An effective hybrid DE-based algorithm for multi-objective flow shop scheduling with limited buffers", *Computers & Operations Research*, Vol. 36, pp. 209-233, 2009.
[34] Batenburg V. and Gultyaev P., "An APL-programmed genetic algorithm for the prediction of RNA secondary structure", *Journal of Theoretical Biology*, Vol. 174, No. 3, pp. 269-280,1995.
[35] Blazewicz J., Formanowicz P., Kasprzak M., Markiewicz W.T. and Swiercz A., "Tabu search algorithm for DNA sequencing by hybridization with isothermic libraries", *Computational Biology and Chemistry*, Vol. 28, No. 1, pp. 11-19, 2004.
[36] Deb K., Pratap A., Agarwal S. and Meyarivan T., "A fast and elitist multi objective genetic algorithm", *IEEE Trans. on Evolutionary Computing*, Vol. 6, No. 2, pp. 182-197, 2002.

**Mohadeseh Soleimanpour** received the BS and MS degrees both in communication engineering from the Bahonar University of Kerman, Kerman, Iran, in 2008 and 2011, respectively; she is currently a PhD candidate in Bahnonar University of Kerman. Her research interests include, image processing, wireless communications and soft computing.

**Siamak Talebi** received B.S. and M.S. degrees, both in Communication Engineering, from Isfahan University of Technology, in 1989 and 1992 respectively and a Ph.D. degree from the University of London (King's College), in 2001. He is currently with the Department of Electrical Engineering at Shahid Bahonar University of Kerman, in Iran. He is also with the Advanced Communications Research Institute at Sharif University of Technology, Tehran, Iran. His research interests are wireless communications, cognitive radio, MIMO-OFDM and also video and image coding.

**Hadi Azadi-Motlagh** received the BS degree from Iran Jondi-Shapour Univeesity of Dezful, Dezful, Iran, in 2009, the MS degree from the Bahonar University of Kerman, Kerman, Iran 2011, in communication engineering. His research interests are in the areas of wireless communications and image processing.