myjournal manuscript No.
(will be inserted by the editor)

Genetic Algorithms for Optimality of Data Hiding in Digital Images

Santi P. Maity[1], **Malay K. Kundu**[2⋆]

[1] Department of Information Technology, Bengal Engineering and Science University, Shibpur Howrah-711103, India e-mail: santipmaity@it.becs.ac.in

[2] Center for Soft Computing Research and Machine Intelligence Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata-700 108, India e-mail: malay@isical.ac.in

Received: 30.1.2008 / Revised version: 31.03.2008

Abstract This paper investigates the scope of usage of Genetic Algorithms (GA) for data hiding in digital images. The tool has been explored in this topic of research to achieve an optimal solution in multidimensional nonlinear problem of conflicting nature that exists among imperceptibility, robustness, security and payload capacity. Two spatial domain data hiding methods are proposed where GA is used separately for (i) improvement in detection and (ii) optimal imperceptibility of hidden data in digital images respectively. In the first method, GA is used to achieve a set of parameter values (used as Key) to represent optimally the derived watermark in the

Send offprint requests to:

⋆ *Present address:* Insert the address here if needed

form of *approximate* difference signal used for embedding. In the second method, GA is used for finding out values of parameters, namely reference amplitude (A) and modulation index (μ) both with linear and non linear transformation functions, for achieving the optimal data imperceptibility. Results on robustness for both the methods against linear, non linear filtering, noise addition, and lossy compression as well as statistical invisibility of the hidden data are reported here for some benchmark images.

Key words Digital data hiding, GA, optimal detection, security, modulation functions

1 Introduction

On one hand the digital information revolution and the thriving progress in network communications offer benefits of almost noise free communication, the ease of editing and the Internet distribution of digital multimedia data. On the other hand the users of digital media are under threat due to the growing concern of copyright infringement, illegal distribution, unauthorized tampering and security in communication. Data hiding that deals with an imperceptible embedding of an auxiliary data in the digital media becomes a potential solution to the latter class of problems over the last decade [1, 2]. Several data hiding methods have been developed for audio, image, video and graphics etc. and are also reported in literature [3–5].

Although data hiding is a common name, steganography and digital watermarking are the two popular terms where the former establishes a covered information channel in point-to-point connection, the later does not necessarily hide the fact of secret transmission to third party. It is found that the degree of requirement may vary based on different applications but the essential requirements of image data hiding, in general, are visual imperceptibility of the hidden data, security against statistical analysis and robustness to non-malicious operations that a communication channel is to face. The processing may include compression for efficient storage and transmission, mean/median filtering for the purpose of noise cleaning. However, the degree or depth of the signal processing operations should be restricted to a level so that the stego/watermarked-object must preserve its commercial value.

Digital data hiding is a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, information theory, cryptography and computer science etc [6]. Soft computing is one subbunch of computer science which may be used to achieve tractable, robust, low cost, optimal and adaptive solutions in data hiding problems. Fuzzy Logic (FL), Rough Sets (RS), Artificial Neural Networks (ANN), Genetic Algorithms (GA) and Support Vector Machine (SVM) etc. are the various components of soft computing and each one offers specific attributes [7]. In data hiding problem, GA may be used for optimizing the fundamentally conflicting requirements of imperceptibility, security and robustness. Neural

network may be used to design robust watermarking for images to take advantages of relatively easy algorithmic specification, pattern mapping and classification. The feasibility of Support Vector Machine (SVM) may be explored to determine automatically where the significant blocks are and to what extent the intensities of the block pixels can be modified [8,9].

Research of data hiding in digital media reports that there exists different trade off relations. For example, if watermark information is embedded in low frequency bands of the cover data, visual quality will be degraded but robustness against lossy compression is increased. Similarly, watermark embedding in high frequency bands of the cover may preserve visual quality but they will be lost even after moderate compression operation [10]. This suggests to choose middle frequency bands in order to make a good trade-off between data imperceptibility and robustness against lossy compression operation although the designated middle frequency bands are not well defined. Similar conflicting situation also arises with the increase in payload capacity which affects visual and statistical invisibility of the hidden data along with robustness performance. These requirements form a multidimensional nonlinear problem of conflicting nature. Most of the data hiding algorithms developed so far focus on single requirement or provide suboptimal solution to meet a group of requirements based on the applications. To resolve the conflicting nature, Genetic Algorithm (GA), like an efficient search for optimal solutions in many image processing and pat-

tern recognition problems [11], may find a potential usage in this topic of research but in reality the usage of the tool has been explored very little.

This paper investigates the scope of usage of GA in two different data hiding applications. In first application which is intended to serve steganographic purpose, GA is used to achieve a set of parameter values (used as key) to represent optimally an approximation of the difference signal (D) that is obtained by subtracting the pixel values of the auxiliary images (messages) from that of the pixel value of the cover image. The approximated difference signal with its proper embedding strength is added to the respective cover data. Experiment results show that the hidden data is secured against statistical analysis and robust to various nonmalicious operations. In second application which is intended to serve watermarking purpose, GA is used to find two parameter values, namely reference amplitude (A) and modulation index (μ) in linear and nonlinear transformation functions used to modulate auxiliary message. Image regions with relatively low information content and having pixel values in the lower and the upper portion of the dynamic range are used for data hiding as the characteristics of human visual system (HVS) are less sensitive to the change at these two ends. Experiment results show that parabolic function offers higher visual and statistical invisibility and reasonably good robustness, whereas, linear function offers higher robustness with reasonably good invisibility. Power-law function neither provides good resiliency nor imperceptibility.

The rest of the paper is organized as follows: Section 2 describes review of the related works, limitation and scope of the present work. Section 3 discusses mathematical analysis of the problem. Section 4 describes proposed data hiding techniques. Section 5 presents performance evaluation separately for the both data hiding methods. Conclusions are drawn in section 6 along with scope of future work.

2 Review of related works, limitations and scope of the present work

This section discusses few soft computing based data hiding methods in order to highlight the effectiveness of this class of tools for performance improvement in data hiding. The objective of this review is to discuss merits and limitations of the existing works, scope of the present work and finally to compare the performance of this work with respect to the some of the related existing works.

2.1 Review of the related works

Wang et al. [12] proposed an algorithm to embed secret messages in the moderately significant bit of the cover images. A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. A local pixel adjustment process (LPAP) is used to improve the image quality of the stego-image. The weakness of the local pixel adjustment process is pointed out in [13]. Wang et al.[14] also proposed a data

hiding scheme by optimal LSB substitution and genetic algorithm. Using the proposed algorithm, the worst mean-square-error (WMSE) between the cover image and the stego image is shown to be 1/2 of that obtained by the simple LSB substitution. These LSB based data hiding methods mostly satisfy imperceptibility requirement but their robustness performances against non-malicious signal processing operations are not satisfactory.

Soft computing techniques are also used in additive watermarking in order to increase robustness performance. Neural networks have been applied to analyze the characteristics of digital image. Back propagation neural network (BPN) model is used in [15] where first nine AC DCT coefficients are the input vectors and the twelfth AC coefficients is the output vector. The weight values can be modified by the training set according to the approximate errors and binary watermark is embedded by applying the concept similar to that of pixel value difference. Similar concept is also used in [16] to embed binary watermark in spatial domain of color image where the image owner collects a set of training patterns to train a neural network. The training pattern is the difference between the intensity of the blue component of the central pixel and the others within the window. Each training pattern contains 9 input vectors and 1 output vector. Legal image owner can use the trained neural network to extract watermarks.

A novel watermarking scheme for the image data using neural networks is also developed based on discrete wavelet transform (DWT)[17]. A coordinate set S is selected from DWT decomposition using a pseudo-random

noise generator (PRNG). A training set is constructed to train the network where each training pattern contains eight input vectors and four expected outputs. The trained network is used to embed watermark. In [18], an empirical model is set up by training a support vector machine (SVM) to classify blocks of pixels from an image and determines the ranks of the blocks in accordance with the perceptual significance blocks. After training, an SVM is constructed to extract the feature of the test block. The SVM and classification regulations must be kept secret by the image owner.

Genetic algorithm is also used for optimizing the fundamentally conflicting requirement in data hiding. Huang et al. [19] proposed progressive watermarking where GA is used to find the optimal frequency bands for watermark embedding into DCT based watermarking system, which can simultaneously improve security, robustness and visual quality of the watermarked image. GA is used to choose the DCT coefficients under certain attacks in every iteration and cost function is developed from the combined contribution of imperceptibility and robustness measure. The similar cost function is also used in spatial domain watermarking using GA where binary watermark is embedded by pixel value difference of mean gray values of a neighborhood [20]. The GA trained result is seen as a secret key and is used in the embedding and the extraction process of watermark information.

2.2 Limitation of the existing works

The discussion in the previous section indicates that soft computing tools find a potential usage to select proper data embedding regions in the cover data, to provide an optimal solution in order to make a better trade-off between imperceptibility and robustness, to increase security in the hidden data etc. However, there are some disadvantages and limitations in the existing soft computing based data hiding methods. We highlight some of the points, in general, rather than mentioning the limitations of individual method.

The main drawback in the proposed GA based data hiding methods lies in the selection of embedding region which is obtained based on pseudo random key and is trained with respect to some neighborhood property to meet imperceptibility requirement. However, this does not offer always better imperceptibility as perceptually significant/non-significant regions not necessarily be considered in the selection process and the knowledge of the cover image characteristics and message to be embedded are not coupled properly. Moreover the existing methods do not ensure statistical invisibility of the hidden data and is not also reported. The other drawback is associated with the cost function which is developed based on the combination of imperceptibility and robustness. The objective functions used to measure these properties vary significantly by numerical values. The varieties of attacks make difficult for equal contribution of imperceptibility and robustness in cost function even if robustness measure is scaled by a factor.

A better cost function may be developed if imperceptibility is measured using mean structural similarity index (MSSIM) (which is having maximum value '1') rather than usage of PSNR (Peak signal-to-noise ratio) or MSE (Mean squared error). The use of MSSIM makes compatibility with NCC (normalized cross correlation) having the maximum numerical value '1' and may be used effectively as imperceptibility measure.

The other main drawback of neural network based data hiding techniques lies in time-consuming training of a neural network and the training process is subtle. Similar problem also occurs as GA need more time to generate a secret key for embedding and extraction. The problem is intensified significantly if more number of attacks are considered to develop the cost function. The other drawback for the existing methods is the lack of proper mathematical modeling. As a result it is difficult to predict imperceptibility and robustness apriori and performance is justified mostly by the experimental results.

2.3 Scope of the present work

In this work we develop two data hiding methods in digital images intended for optimal detection in steganography [21] and optimality in imperceptibility and robustness in watermarking [22]. GA is used outside the data hiding process in order to overcome time complexity problem and is used to find optimum parameter values for improved detection and optimum invisibility. The contribution of the work is briefly described as follows:

(i) In the first data hiding method, GA is used to achieve a set of parameter values (used as Key) to represent optimally the difference signal (D) that is obtained by subtracting the pixel values of the auxiliary images (messages) from that of the pixel values of the cover image. The approximate difference signal with its proper embedding strength is added to the respective cover data. The embedding strategy ensures visual and statistical invisibility of the hidden data. The usage of GA, with the increase of iterations, improves detection of the hidden data.

(ii) In the second data hiding method, GA is used to find two parameter values, namely reference amplitude (A) and modulation index (μ) in linear and non linear transformation functions used to modulate the auxiliary message. Experiment results strongly conform mathematical analysis to select proper modulation function so that simultaneously better visual and statistical invisibility of the hidden data as well as robustness against common signal processing operations can be achieved.

3 Mathematical analysis of the data hiding problem

This section describes required mathematical analysis of the two data hiding methods to be described in the next section. The data hiding methods are denoted here as Method 1 and Method 2.

3.1 Method 1:Optimal detection and stego test

Different data hiding applications require different payload, typically varying from a few bits in access control, up to at most one hundred bits in authentication and fingerprint problems, may demand much higher payload capacity for information-hiding applications. The last application can be used for covert communication and objective is to embed data in such a way without compromising much of image fidelity and decoding reliability. In additive embedding process, data hiding is accomplished by adding a scaled version of the auxiliary message to the host data. Image fidelity is degraded with the increase in payload capacity and embedding strength. The higher value of embedding strength, at the cost of greater visual distortion, increases reliability of decoding i.e. robustness against signal processing operations.

One possible solution to cope up this trade-off like problem is to map the auxiliary message signal to a difference signal. This is formed by selecting the embedding region within the cover signal so that auxiliary message forms a lower distance difference signal. Now the difference signal can be approximated to less number of signal points and be added with higher embedding strength so that visual distortion of the cover can be set to an acceptable value. This essentially means that higher payload capacity is other way represented by higher embedding strength of less signal points for a given visual distortion of stego images. Decoding of message is accomplished by extraction of an approximate difference signal and inverse

process will regenerate the message signal. The reliability of the decoding process depends on how faithfully the difference signal is approximated and regenerated. The best decoding is possible if the entire difference signal is embedded which significantly degrades the visual quality distortion of the stego images. To reiterate the problem, visual quality distortion of the stego images caused due to higher payload capacity can be reduced by embedding an approximated *difference* signal of *less signal points* but at the same time robustness is improved due to relatively higher embedding strength. Thus important point arises how to select those N- signal points that regenerate the M-point difference signal faithfully where $N \ll M$.

The above problem can be stated mathematically as follows: Given an M-point difference signal (D), how an approximate signal ($D^{'}$) be generated using N- signal points where $N \ll M$ and $D^{'}$ is close resemblance of D. One way to regenerate better approximation signal is to use higher order interpolation but in that case computation cost increases exponentially with the order of interpolation. Linear interpolation is a good compromise between the computation cost and better approximation for the regenerated signal. In such case, it is the important point to find which N-points would generate better approximation and how N-values affect this approximation function. This is an optimization problem and GA finds application to yield optimal solutions. We define a parameter called *payload efficiency* (C) which is the ratio of N and M (N/M) and the choice of low value of C otherway indicates better data imperceptibility as a given payload is met by embedding

less number of signal points. It is to be noted here that the novelty of this type of principle used for development of data hiding algorithm is justified by improved detection reliability at relatively low payload efficiency.

3.1.1 Steganalysis based on higher order statistics Farid proposed a universal blind steganalytic detection method [23] based on higher order statistics of natural images. We briefly describe the algorithm in two steps as follows: (1)Extraction of a set of statistics, called the feature vectors, for each investigated image. (2) Formation of a classification algorithm to separate untouched images from stego-images on the basis of their feature vectors.

Formation of feature vectors

The feature vector, for a certain image, is formed using the first four normalized moments namely Mean, Variance, Skewness and Kurtosis of the wavelet coefficients of vertical ($v_i[x, y]$), horizontal ($h_i[x, y]$), and diagonal ($d_i[x, y]$) subbands at scales $i = 1, 2, 3....n$. Thus we have total 4.3. (n-1) elements of the feature vector f for the test image.

The remaining elements of f are derived from the Error Statistics of an optimal linear predictor. The prediction for a specific subband coefficient is performed considering the 4 neighboring coefficients, the corresponding in the courser scale of the same orientation and coefficients of subbands of other orientations (and scales).

The predicted value for the vertical subband $v_i[x, y)]$ is given by

$$v_i^{'} = w_1 v_i[x-1, y] + w_2 v_i[x+1, y] + w_3 v_i[x, y-1] + w_4 v_i[x, y+1]$$

$$+w_5 v_{i+1}[x/2+y/2]+w_6 d_i[x,y]+w_7 d_{i+1}[x/2,y/2] \quad (1)$$

where w_k denotes the predictor coefficients. The other two subbands $h[x,y)]$ and $d[x,y)]$ can be predicted in the same way The optimal predictor coefficients $w_{k,opt}$ are determined for each subband so that the mean squared error within each is minimised. The log error in the linear predictor is then given by:

$$e_{v_i}{}^{log}[x,y] = \log_2(v_i[x,y]) - log_2(v_i^{'}[x,y]) \quad (2)$$

where $v_i[x,y]$ is obtained by inserting $\mathbf{w_{k,opt}}$ into equation (1), yields the Log Error. The mean, variance, skewness, and kurtosis of the Log Error of each subband form the remaining 4.3.(n-1) elements of f.

Classification Algorithm

The classification algorithm called the Fisher Linear Discriminant (FLD) analysis is used to classify a new image by means of its feature vector. The FLD algorithm is first trained with feature vectors from untouched and stego-images. The algorithm determines a projection axis by means of this training set to project the 24.(n-1)-dimensional space of feature vectors into a one dimensional subspace. The projected feature vector **f** is referred to as the Detection Variable **d**. New feature vectors obtained from new images are classified by thresholding **d**. If d is greater than a certain value, the image is classified as stego, if not, it is classified as untouched.

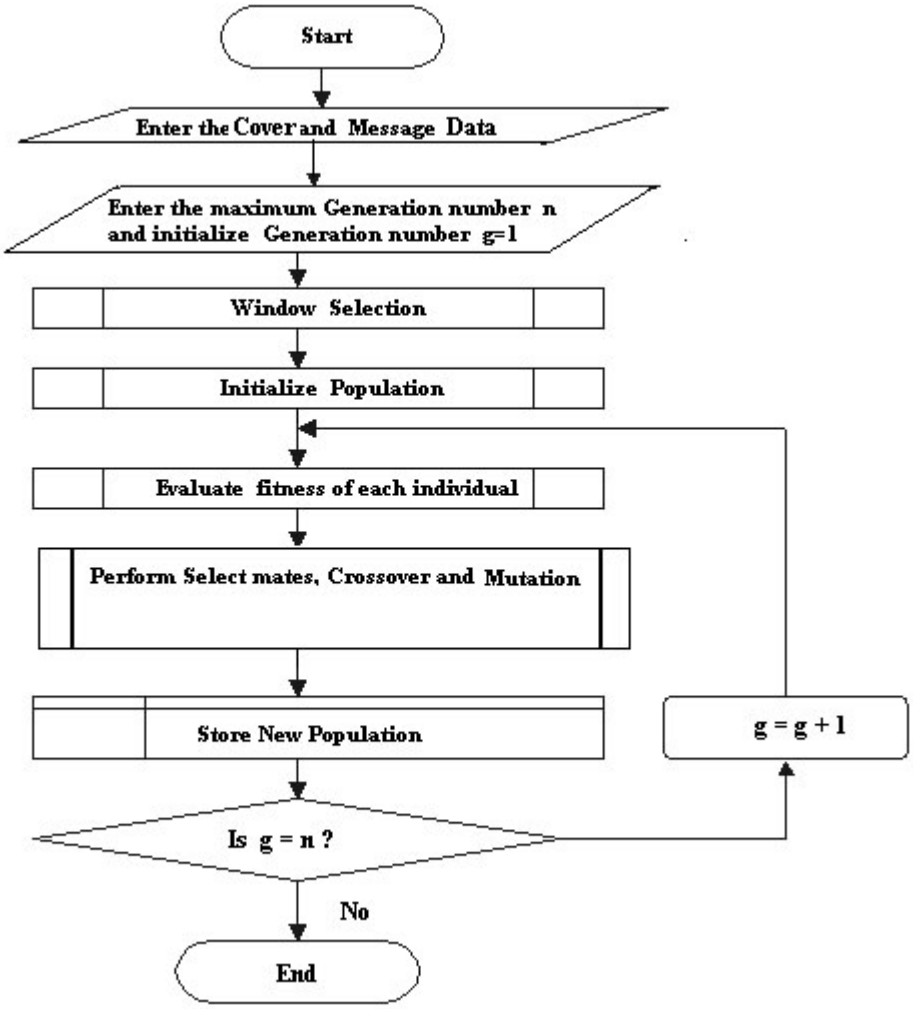

Fig. 1 Flowchart for the main module of the proposed work:Method 1

3.2 Method 2: Modulation function and calculation of parameters

This method focuses on optimal imperceptibility and robustness of the hidden data. The cover and the auxiliary message are chosen as gray level images. The auxiliary message (watermark) is modulated using suitable transformation functions to match the characteristics of the cover image re-

gions. Distortions are then created over stego image to simulate the behavior of a noisy channel.

The power-law function $X^{'} = A(X + \varepsilon)^{\mu}$ which is widely used for image enhancement operation is considered as modulation function. Here X denotes the pixel value in auxiliary message and transformation function modulates X to $X^{'}$, the pixel value of the cover image selected for embedding. Two other transformation functions, one is linear transformation function of the form $X^{'} = A(1 + \mu X)$ and other one is parabolic function of the form $X^{'} = A(1 + \mu\sqrt{X})$, are compared for their suitability on imperceptibility, security and robustness issues of data embedding. The following subsections describe how to calculate the range of parameter values.

Calculation of A

The modulation function is as follows:

$$X^{'} = A(X + \varepsilon)^{\mu} \tag{3}$$

Differentiating $X^{'}$ with respect to X, we get

$$dX^{'}/dX = A\mu(X + \varepsilon)^{\mu-1} \tag{4}$$

Here $dX^{'}/dX$ is positive provided $A > 0$, $\mu > 0$ and $(X + \varepsilon) > 0$, which implies $X^{'}$ increases monotonically with X. The upper $(U^{'})$ and lower $(L^{'})$ bound of the modulated pixel values are

$$U^{'} = {X_{max}}^{'} = A(X_{max} + \varepsilon)^{\mu} \tag{5}$$

$$L^{'} = {X_{min}}^{'} = A(X_{min} + \varepsilon)^{\mu} \tag{6}$$

The range (Ψ) of the modulated pixel values is given as follows:

$$\Psi = U^{'} - L^{'} = A[(X_{max} + \varepsilon)^{\mu} - (X_{min} + \varepsilon)^{\mu}] \tag{7}$$

The relation shows that for large A value, the span of the modulated pixel values (Ψ) will be large leading to smaller probability of matching between the modulated message and the embedding regions. This in turn suggests to select the lower value of A for better imperceptibility. The small span (Ψ) is also possible for large A value provided very small value is selected for μ. But it is shown in the detection process that small value of μ will make the auxiliary message vulnerable to elimination in noisy transmission media. Similar argument also holds good for the value of A. The value of A depends on selection of the auxiliary message as well as regions selected for embedding. As rule of thumb A is selected as

$$A = X^{'}_{mode}/(X_{mode} + \varepsilon)^{\mu} \tag{8}$$

where $X^{'}_{mode}$ and X_{mode} respectively denote the mode of the gray values for the embedding regions and the auxiliary messages.

Calculation of μ

Power-law transformation suggests if μ value is taken small ($\mu < 1.0$) keeping A constant, auxiliary message is mapped into a narrow range of gray values. This fact is also supported by equation (7). Confinement of gray values inside a narrow range increases the probability of matching between the

modulated message and the data embedding region. But very small value of μ degrades the quality of the detected message to a non-recognizable form even after a very small image distortion. The upper and the lower value of μ are calculated as follows:

It is found that $X^{'}$ is a monotonically increasing function of X. The value of ε, acts as offset value in image display, is set to (~ 0.01). From equation (3), we write

$$X^{'}_{max} = A(255 + 0.01)^{\mu} = A(255.01)^{\mu}$$

The maximum X value is taken 255 for monochrome gray level image. The corresponding μ value is designated as μ_{max} and is related with X_{max} and A as follows:

$$\mu_{max} \simeq \frac{\log X^{'}_{max} - \log A}{\log 255}$$

Similarly, μ_{min} value can be written as follows:

$$\mu_{min} \simeq \frac{\log X^{'}_{min} - \log A}{\log 0.01} = \frac{\log A - \log X^{'}_{min}}{2.0}$$

The value of μ will be positive if A lies between X_{max} and X_{min} where the later values represent the maximum and the minimum gray values of the embedding regions respectively.

4 Proposed data hiding methods

This section describes two data hiding methods in digital images. We describe both data hiding methods one after another.

4.1 Method 1: Data embedding for optimal detection

The total process of data embedding and decoding consists of three stages. These are Stage 1: Selection of data embedding regions and formation of difference matrix, Stage 2: Generation of set of points using GA to optimally represent the difference matrix followed by data embedding, Stage 3: Message retrieval. Fig. 1 represents the flowchart for the main module of the proposed work.

Stage 1

The choice of cover images is important and influences the security in a major way. Images with a low number of colors, computer art, images with a unique semantic content, such as fonts, should be avoided. Some data hiding experts recommend grayscale images as the best cover-images. We consider gray scale image as cover and the similar type image like text information as message signal since it can preserve contextual information even after various signal processing operations. Steps for the selection of embedding region are as follows.

Step 1 : Input gray scale images as cover and message signal.

Step 2: Setting of an appreciable percentage for matching criteria (say 85

percent)

Step 3 : Selection of a region from the cover equal in the size to that of message signal.

Step 4 : Comparison of variation of the pixel values between the cover and the message signal.

Step 5 : Repetition of the above process by dynamically selecting windows all over the cover image.

Step 6 : Once the percentage matching criteria is satisfied, the process terminates, otherwise, it is continued till the end of the cover image.

Step 7 : Output: (1) If percentage matching criteria is satisfied, then returns the Difference Matrix to ensure a smooth image with little variations. (2) If no matching region is found, returns a null matrix denoting failure of finding the specified percentage matching region.

Stage 2

The main objective is to find an optimal set of points using GA so that an approximate version of difference signal can be generated.

1. Initialization of population: Chromosomal representation of the parameter values. The initial population is formed by taking almost equispaced x-y data points with small perturbations.

2. Select Mates: Objective : To select, most of the times, the best fitted pair of individuals for crossover.

Step 1 : Input : Population

Step 2 : Best fitted pair of Individuals are chosen by Roulette-wheel selec-

tion process by adding up fitness values of the individuals to get *Sumfitness*

Step 3 : Then randomly select Individuals to cross 50% of the *Sumfitness* value in a cumulative way

Step 4 : The particular Individual which crosses the 50% criteria in the Cumulative process, is chosen to be one of the mating pool pair.

Step 5 : This process is again carried on to find another Individual of the mating pool

Step 6 : Output : Pair of Individuals or mating pool

3. Crossover: Objective: To find the Crossover site and to perform crossover between the Mating pool pair to get new pair of more fitted Individuals.

Step 1 : Input: Mating pool pair

Step 2 : Finding the crossover site in a random manner

Step 3 : Exchange the portions lying on one side of crossover site of those mating pool pair

Step 4 : Output: New pair of Individuals

4. Mutation: Objective: To mutate or change a particular bit or allele in a Chromosome with a very small probability.

Step 1 : Choose a very small mutation probability

Step 2 : Depending upon that probability value, change a bit from '1' to '0' or '0' to '1'

Step 3 : The bit position selected for mutation is the Crossover site

5. Objective function: Objective : To estimate the fitness value of an Individual

Step 1 : Input: Population

Step 2 : On each Individual of the Population apply 2-D interpolation technique to approximate the original matrix

Step 3 : The absolute mean error is evaluated by subtracting the interpolated matrix from the original matrix

Step 4 : The inverse of that absolute mean error is considered to be the fitness value of that particular Individual

6. Data embedding: The N-points approximated difference matrix ($D^{'}$) thus obtained is then multiplied by proper embedding strength (K), and added to the respective pixel values of the cover image (C). The stego image can be obtained as follows:

$$S = C + K.D^{'} \tag{9}$$

Stage 3

The final stage of the algorithm is the retrieval process of the message. It is assumed that stego-image has undergone some changes due to non-malicious signal processing operations. An estimated version (D_{est}) of approximated difference signal ($D^{'}$) is obtained using linear interpolation technique among the N-points grayscale values calculated by GA. The approximate cover image matrix C_{app} is then calculated using the Stego-image S and D_{est} as follows:

$$C_{app} = S - K.D_{est} \tag{10}$$

The message can be retrieved from the following relation:

$$L = C_{app} - D_{est} \tag{11}$$

where $D_{est} = K.D^{'}$.

4.2 Method 2:Data embedding for optimal invisibility and robustness

GA for data hiding

Let us analyze the use of GA in the present data hiding method:

(1) Chromosomal representation of the parameter values, namely the reference amplitude (A) and the modulation index (μ) associated with the problem.

(2) Creation of an initial population of chromosomes for possible solutions by using random binary strings of length pq where p represents the number of parameters and q are the bits assigned for each parameter.

(3) To quantify the closeness measure among pixel values over sub image or image, average Euclidean distance is considered here as fitness function. This fitness function considers imperceptibility of the hidden data directly. It is to be noted that different linear and non-linear functions are tested here for modulating the message signal in order to meet robustness criterion. Thus the usage of the average Euclidean distance together with various modulation functions meet both the imperceptibility and robustness requirement simultaneously. The fitness function may also be designed by combined contribution of robustness and imperceptibility measure as used in [20].

The value of pay-off function based of Euclidean distance can be expressed mathematically as follows:

$$F(A,\mu) = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}[S_{ij} - e_{ij}(A,\mu)]}{N^2} \tag{12}$$

where S_{ij} is the gray value of (i,j)-th pixel of the embedding region, $e_{ij}(A,\mu) = A(X_{ij}+c)^{\mu}$, is the gray value of (i,j)-th pixel of the message after modulation and N^2 is the total number of pixels in the embedding regions as well as in the auxiliary message.

(4) According to De Jong's elitist model [24], the best fit string obtained is included in the new population to preserve the best structure in the population.

(5) Although the high mutation probability leads to exhaustive search which may result in better imperceptibility at higher computation cost. Here moderate value of mutation probability is chosen in order to achieve imperceptibility at comparatively lower cost.

Message hiding and recovery

This method models data hiding as conventional amplitude modulation of communication where various linear and nonlinear functions are used to modulate watermark. The pixel values of the watermark information are similar to the amplitude of the unmodulated carrier although the former is not fixed unlike the latter. The pixel values of the watermark image are modulated in such a way so that they match with the pixel values of the embedding region in the cover image as approximately as possible. The embedding region from the cover image can be selected from its histogram on

the basis of higher frequency of occurrence in pixel values in either end or on the basis of the histogram of the difference matrix. The message modulated by transformation function using GA replaces the selected regions of the cover image.

Data recovery process uses inverse transformation function that maps $X^{'}$ into X and thus message is recovered. If power-law, linear and parabolic functions are used for message modulation, extracted message can be represented respectively as follows:

$$X = (X^{'}/A)^{1/\mu} - \varepsilon \tag{13}$$

$$X = (1/\mu A)(X^{'} - A) \tag{14}$$

$$X = 1/(\mu A)^2(X^{'} - A)^2 \tag{15}$$

Differentiating equations (13),(14) and (15) with respect to $X^{'}$ the following equations are obtained respectively,

$$dX/dX^{'} = (1/\mu)(1/A)^{1/\mu}(X^{'})^{1/\mu - 1} \tag{16}$$

$$dX/dX^{'} = 1/\mu A \tag{17}$$

$$dX/dX^{'} = 2(X^{'} - A)/(\mu A)^2 \tag{18}$$

$dX/dX^{'}$ denotes the change of X with respect to the change of $X^{'}$ i.e. a measure of noise immunity in the detection process. The large values of A and μ are preferable for reliable decoding whereas small values of the same are desirable for better imperceptibility. Lower value of $dX/dX^{'}$ indicates better reliability in detection process.

5 Performance evaluation

This section presents simulation results to show the performance of the proposed two data hiding methods one by one. The experiment is carried out here for the cover image of size (256×256), 8 bits/pixel and the auxiliary message/watermark is also a gray scale image where the size and the range of gray values vary depending upon the situations. The performance results for both the data hiding methods are reported here for a watermark of (64×64), 4 bits/pixel gray scale image. The visual quality of the watermarked image is represented by peak signal-to-noise ratio (PSNR). Similarly, the visual quality of the extracted message/watermark is represented by mutual information $I(W; W^{'})$ where random variables W and $W^{'}$ represent the watermark image and its decoded version extracted from the stego/watermarked image (Y). We consider data embedding in the host data and the extraction of the auxiliary message/watermark at the user end as a digital communication problem and hence mutual information is used as an objective measure [25]. Although it is difficult to correlate the recognizability of the watermark pattern with $I(W; W^{'})$ values, the experiment results suggest that $I(W; W^{'})$ value 0.07 can be considered as threshold of recognizability for the watermark image shown in Fig. 2(b). The experimental conditions for both the GA based data hiding methods are as follows: Size of population is 20, number of generations are 800, probability of cross-over per generation is 0.95, probability of mutation is 0.005.

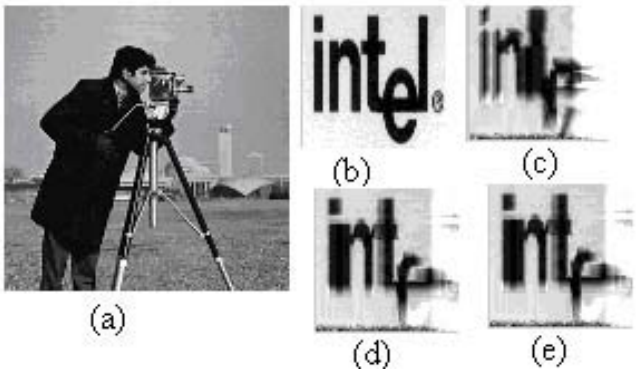

Fig. 2 (a) Watermarked image; (b) watermark image; (c)-(e) retrieved messages after 100, 200 and 400 iterations respectively

5.1 Performance evaluation of method 1

The efficiency of the proposed algorithm is tested by embedding different messages in several cover images like Cameraman (results reported), Black bear, Bandron [26] etc. and the messages are extracted from the various noisy versions of the stego images. The security of the hidden data is represented numerically by relative entropy distance (Kulback Leibler distance)[27] apart from the use of Farid's steganalytic test. The stego image is shown in Fig. 2(a) and PSNR value for the watermarked image is 39.33 dB. The security of the hidden data is 0.00124. As the number of generations are increased from 100, 200 to 400, observation of Figs. 2(c), 2(d) and 2(e) reveals the fact that the visual recognizability of the retrieved watermark images increase more and more close to the original images. The $I(W;W^{'})$ values for the extracted messages are 0.0894, 0.1012 and 0.1252 respectively. We emphasize on subjective quality for the recognizability of the extracted

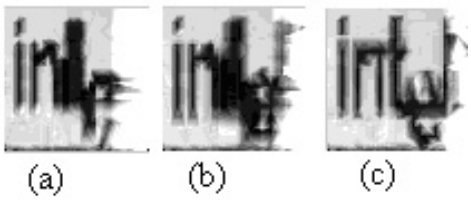

Fig. 3 Robustness performance of median filtering; (a),(b) and (c) indicate retrieved watermark messages after 50, 100 and 150 iterations respectively

message as well as objective measure. The improvement in decoding is borne out by the property of GA which produces better solutions as the number of generations/iterations are increased. It is obvious that the greater be the length of the secret key, better is the watermark detection performance i.e. the use of more number of signal points offers better robustness performance at the cost of large overhead. We report here all the experiment results for the secret key of length 100 i.e the number of signal points N considered here are (10×10).

Sometimes various linear and nonlinear filtering are used to remove noise from the images. Median filtering is one nonlinear filtering that removes noises but preserves edge information. Fig. 3 shows the retrieved watermark messages from the median filtered version of the watermarked images. The stego image is filtered using (5×5) window. Fig. 3 show how the quality of the retrieved messages are improved with the number of iterations although the number of signal points N (100) remain the same. Figs. 4 (a),

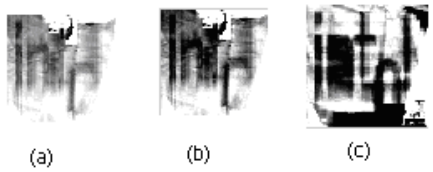

Fig. 4 Robustness performance against JPEG compression at quality factor 60; (a), (b) and (c) indicate retrieved watermark messages after 50, 100 and 150 iterations respectively

4(b) and 4(c) show the watermark images extracted from the compressed stego images at quality factor 60 using the approximate estimated difference signal after GA iterations of 50, 100 and 150 respectively. Once again, it is shown that visual recognizability for the extracted images improve with the increase of number of iterations although the over all robustness performance against compression operation is not satisfactory like transform domain embedding methods due to obvious reasons. Fig. 5 shows the graphical representation of detection performance with the number of iterations for different payload efficiency i.e 'C' values. Simulation results show that detection performance is improved with the increase of 'C' values i.e. with the increase in embedding of more signal points for the approximated difference signal. It is also shown that for a given 'C' value detection performance is also improved with the increase of number of iterations. Fig.6 shows the stego-test results. As we observe, this stego-test does not place the test image within the cluster for sample stego-images. Therefore, the test cannot

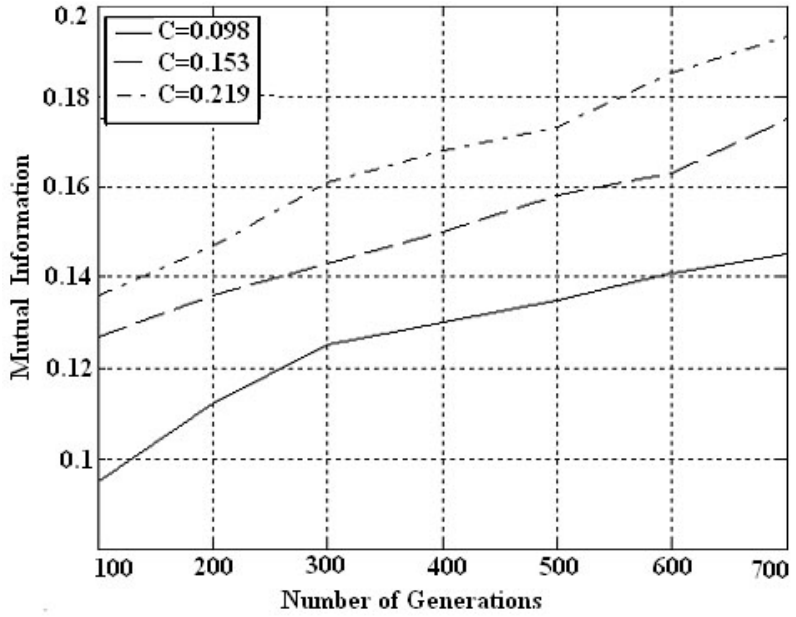

Fig. 5 Detection improvement with the number of iterations/generations for different payload efficiency 'C'

Fig. 6 Stego-test; Black cross–stego test image using proposed algorithm; (b)Colour circles–Sample stego images after various operations; (c)red square–untouched image

decide with certainty that the test image is actually a stego-image. This establishes the security of the proposed algorithm against Farid's steganalytic technique involving higher-order statistics. The security against statistical analysis for the hidden data is achieved as difference signal is embedded rather than the original watermark. Moreover, the embedding of the compact or approximated difference signal further causes very small change in higher order statistics of the pixel values in the embedding regions.

5.2 Performance evaluation of method 2

The efficiency of the proposed algorithm is tested for different transformation functions used to modulate the message signal. Fig. 7(a)-7(p) show the watermarked images obtained by using such modulation functions, extracted watermark images after mean, median filtering and JPEG compression operations. Table 1 shows the imperceptibility, security and robustness results where the subscripts 1, 2, and 3 used in the objective measures indicate the results for power-law, linear and parabolic functions respectively. It is shown by the results that imperceptibility-security-robustness performance are increased simultaneously using the GA based data hiding method and performance increases with the increase of number of iterations.

Fig. 8(a) shows the graphical representation of imperceptibility with the number of iterations for the different modulation functions as well as for the method reported in [20] for δ= 10. Simulation results show the use of parabolic function offers better imperceptibility compared to [20], although

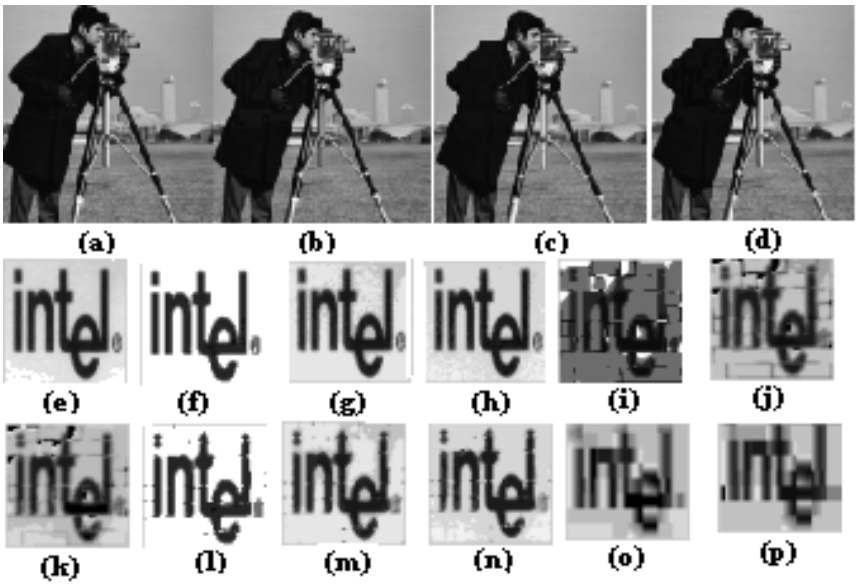

Fig. 7 (a) Cover image; (b), (c), (d) Stego images using power-law (PSNR=41.77 dB), parabolic function (PSNR=51.58 dB), linear function (PSNR= 47. 45 dB) respectively; (e) Auxiliary message; (f), (g), (h) Extracted messages from (b), (c), (d) respectively; (i), (j), (k) Extracted messages from mean filtered stego images when power law, parabolic, linear functions are used respectively after 200 generations; (l), (m), (n) Extracted messages from median filtered stego images when power law, parabolic, linear functions are used respectively after 200 iterations; (o), (p) Extracted messages from compressed (JPEG) stego images (PSNR=31.06 dB) and (PSNR=31.88 dB) at quality factor 70 using linear and parabolic function respectively after 400 iterations.

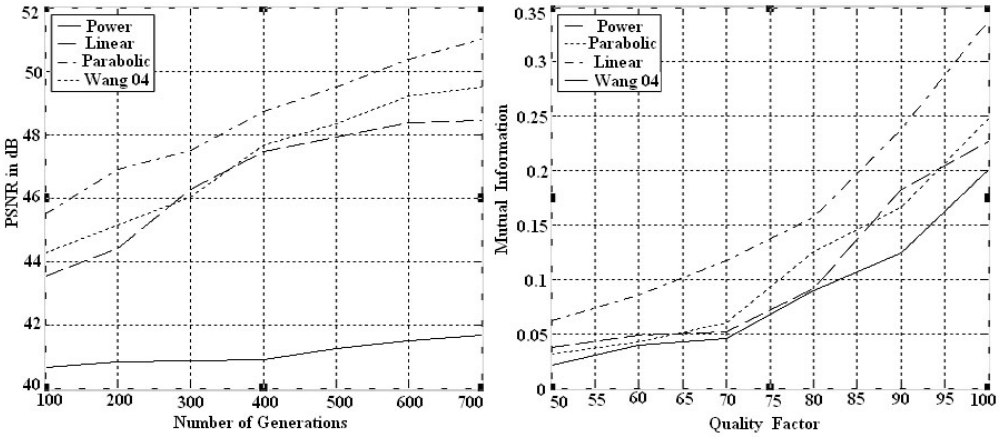

Fig. 8 (a) Imperceptibility represented by PSNR in dB with the number of iteration for different modulation functions; (b) Robustness against lossy JPEG compression operation

the same for [20] is superior compared to the use of linear and power law functions. Fig. 8(b) shows graphically the robustness performance of the proposed data hiding method against lossy JPEG compression operation as well as comparison of the same with [20]. The lower mutual information values for the extracted watermarks in [20] are possibly due to binary watermark signal in which uncertainty in the decoded bit is more compared to the gray scale watermark. Moreover, it is found that visual recognizability of the extracted watermark for [20] is poor below the quality factor 70 while the use of linear modulation function is capable of preserving the same even at quality factor 50. It is also found that robustness performance for other two modulation functions are also better compared to [20].

Table 1 Performance results of different modulation functions

Gen. no.	PSNR, ε value,$I(X;Y)$ $(dB)_1$, (1),value(1)	PSNR , ε value,$I(X;Y)$ $(dB)_2$, (2), value(2)	PSNR , ε value,$I(X;Y)$ $(dB)_3$, (3), value(3)
50	40.56, 0.046,0.15	43.49 ,0.030,0.398	45.42,0.037,0.32
150	40.79,0.045, 0.19	44.36,0.034,0.40	46.74,0.037,0.34
400	40.90,0.041,0.20	47.90,0.036,0.42	48.73,0.036,0.35
600	41.50, 0.039,0.21	48.36,0.037,0.44	50.37,0.025,0.38
800	41.77,0.038, 0.28	47.45,0.040,0.48	51.53,0.023,0.39

Robustness efficiency against mean, median filtering and lossy compression are shown in the respective figures (Fig. 7). Figs. 7(i), 7(j) and 7(k) show the watermark images extracted from the stego-images after mean filtering using (5×5) window and using parameter values obtained after 200 iterations. Similarly, Figs. 7(l), 7(m) and 7(n) show the extracted watermark images after median filtering using (5×5) window and using parameters obtained after 200 iterations. Robustness performance against lossy JPEG compression at quality factor 70 are shown in Fig. 7(o) and 7(p) for the linear and parabolic function after 400 iterations. In all such cases the extracted watermark images are visually recognizable with high mutual information values. Poor robustness in the case of power law function is supported by eqn. (16) where small values of A and μ causes change in $X^{'}$ manifold even for the small change in X. Linear transformation function offers better imperceptibility as large range of message gray values can be mapped to smaller range by choosing the small slope i.e. the product of A and μ. At

the same time better resiliency is achieved since $dX/dX^{'}$ (equation 18) is no way dependent on $X^{'}$ although very small values of A and μ will affect the detection process. Best data imperceptibility and security result is possible in case of parabolic function, as small values of A and μ map wide range of message gray values to the narrow region in the lower range of pixel values of the cover image. Detection reliability in such case is also satisfactory since $dX/dX^{'}$ does not contain $X^{'}$ with power term of A and μ like power law transformation function, although small values of the parameters affect detection process little more compared to linear transformation function.

6 Conclusions and scope of future works

This paper investigates the scope of usage of GA for optimality of data hiding in digital images and accordingly two algorithms are proposed. The first algorithm proposes data hiding method with improved payload capacity intended for covert communication. GA is used to achieve a set of parameter values so that faithful decoding of message is possible. Decoding reliability is improved with the increase of number of iterations in GA when the set of parameter values are fixed. The algorithm is proven to be secured against stego-test based on higher order statistics.

The second method proposes an invisible image-in-image communication through noisy channel where linear, power-law and parabolic functions are used to modulate the auxiliary messages. GA is used to find the optimal parameter values, viz. reference amplitude (A) and modulation index (μ)

for data imperceptibility. Experimental results show that parabolic function offers higher visual and statistical invisibility and reasonably good robustness, whereas, linear function offers higher robustness with reasonably good invisibility. Power-law function neither provides good resiliency nor imperceptibility.

Future work may be carried out to extend the proposed concept involving more parameters and more complex system that includes the characteristics of human visual system (HVS) .

References

1. C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, Invisibility and Application Functionalities in Perceptual Watermarking- An Overview, Proc. IEEE,**90,** (2002) 64-77.
2. M. Wu and B. Liu, *Multimedia Data Hiding*(Springer-Verlag, NewYork 2002).
3. Special issue on copyright and privacy protection, IEEE Journal on Selected Areas in Communication (JSCA) **16,** (1998).
4. Special issue on enabling security technologies for digital right management, Proceedings of IEEE, **92,** (2004).
5. J. S. Pan, H. C. Huang and L. c. Jain (Eds), *Intelligent Watermarking Techniques* (World Scientific, Singapore 2004).
6. D. Kundur, Multiresolution digital watermarking: algorithms and implications for multimedia signals, Ph. D thesis, Dept. of Electrical and Computer Engineering, University of Toronto, Canada, 1999.
7. S. K. Pal, A. Ghosh and M. K. Kundu(eds.), *Soft Computing for Image Processing* (Physica Verlag, Heidelberg 2000).

8. C. S. Shieh, H.-C. Huang, F. H. Wang, and J. S. Pan, Genetic watermarking based on transform domain techniques,Pattern Recognition,**37,**(2004)555-565.

9. J. S. Pan, M. T. Sung, H.-C. Huang and B. Y. Liao, Robust VQ-Based digital watermarking for the memoryless binary symmetric channel, IEICE Trans. on Fundamentals of Electronics, Communication and Computer Sciences,**E-87A,**(2004)1839-1841.

10. J. S. Pan, H.-C. Huang, L. C. Jain and W. C. Fang(eds), *Intelligent Multimedia Data Hiding:New Directions*(Springer, Berlin-Heiderber, Germany 2007).

11. S. K. Pal, D. Bhandari and M. K. Kundu, Genetic algorithms for image enhancement, Pattern Recognition Letters,**15,**(1994)261-271.

12. R. Z. Wang, C. F. Lin and J. C. Lin, Hiding data in images by optimal moderately significant-bit replacement, IEE Electronics Letter, **36,**(2000) 2069-2070.

13. C. K. Chan and L. M. Cheng, Improved hiding data in images by optimal moderately significant-bit replacement, IEE Electronics Letter, **37,**(2001)1017-1018.

14. R. Z. Wang, C. F. Lin and J. C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition Letter, **34,**(2001) 671-683.

15. M. S. Hwang, C. C. Chang and K. F. Hwang, Digital watermarking of images using neural networks, Journal of Electronic Imgaging, **9,** (2000) 548-555.

16. P. T. Yu, H. H. Tsai and J.S. Lin, Digital watermarking based on neural networks for color images, Signal processing, **81,**(2001)663-671.

17. C.C. Chang and I. C. Lin, Robust image watermarking system using neural network, *Intelligent Watermarking Techniques*(World Scientific, Singapore 2004) 395-427.

18. C.C. Chang and I. C. Lin, A perceptually tuned watermarking scheme for digital images using supprot vector machines, *Intelligent Watermarking Techniques*, (World Scientific, Singapore 2004)429-457.

19. H.-C Huang, J. S. Pan, Y. H. Huang, and K.-C. Huang, Progressive watermarking techniques using Genetic Algorithms, Circuits, Systems, and Signal Processing,**8,**(2007)58-68.

20. F. H. Wang, L. C. Jain, and J. S. Pan, Genetic watermarking on spatial domain, *Intelligent Watermarking Techniques*, (World Scientific, Singapore, 2004)377-393.

21. S. P. Maity, M. K. Kundu and P. K Nandi, Genetic algorithm for optimal imperceptibility in image communication through noisy channel, 11 th International Conference on Neural Information Processing ICONIP 2004, (LNCS, Springer Verlag,2004) 700-705.

22. S. P. Maity, P. K. Nandi and M. K. Kundu, Genetic Algorithm for improvement in detection of hidden data in digital images, 6th International Conference on Advances in Pattern Recognition, (World Scientific 2007) 164-169.

23. H. Farid, Detecting Steganographic Message in Digital Images, *Dartmouth College,Computer Science*, (TR2001,2001).

24. D. Goldberg, *Genetic Algorithms: Search, Optimization and Machine Learning*, (Addison-Wesley, Reading, M.A., 1989).

25. R. H. Hamming, *Coding and Information theory*, (Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1980).

26. http:// www.cl.cam.ac.uk/ fapp2/watermarking.

27. C. Cachin, An information theoretic model for steganography, Proceedings of 2nd Workshop on Information Hiding. D. Aucsmith (Eds.). Lecture Notes in Computer Sciences, Springer-verlag, USA, **1525,** (1998).