Intelligent Image Watermarking based on Handwritten Signature

Saeid Shahmoradi
Department of computer, college of Engineering technical
Bandar Abbas Branch, Islamic Azad University
Bandar Abbas, Iran

Nasrollah Sahragard*
Department of Electrical and Computer Engineering
University of Hormozgan,
Bandar Abbas, Iran

Ahmad Hatam
Department of Electrical and Computer Engineering
University of Hormozgan,
Bandar Abbas, Iran

***Abstract*—With the growth of digital technology over the past decades, the issue of copyright protection has become especially important. Digital watermarking is a suitable way of addressing this issue. The main problem in the area of watermarking, is the balance between image transparency and resistance to attacks after watermarking, where an increase in either one of them will always cause a decrease in the other. Providing statistical and intelligent methods, is the most common way of optimizing resistance and transparency. In this paper, the intelligent method of genetic algorithm (GA) in watermarking will be examined and also the results of using this method will be compared with the results of a statistical SVD-based method. Also, by combining the issues of watermarking and authentication, a relatively higher security in these two issues can be achieved. In this scheme, the security of watermarking increases through the provision of a new method which is based on the combination of image watermarking with a person's handwritten signature. It must be mentioned that the section of signature recognition is implemented using neural networks. The results from implementing these two methods show that in this area, intelligent methods have a better performance compared to statistical methods. This method can also be used for tasks like passport or national identity card authentication.**

Keywords—intelligent watermarking; genetic algorithm; neural networks; handwritten signature

I. Introduction

With the growth of digital technology over the past decades, sending and storing of electronic media have also increased, because copying data without any loss of quality and with a very small cost has become possible. Therefore, use of digital works without compliance with copyrights, document manipulation and use of forged documents, have found new dimensions. Use of traditional encryption systems made it possible that only a person possessing a key would be able to view an encrypted media text. But even in this condition, after data decryption, it will still be possible to use it illegally. Therefore, traditional encryption methods will not be efficient enough to prevent unauthorized use and malicious attacks. In such circumstances, intangible data embedding for prevention of unauthorized use, has a high commercial potential. Digital watermarking has been introduced to overcome this problem [1]. In watermarking methods, there are a series of requirements which need consideration. Of the most important requirements to mention are watermark transparency, resistance, security and capacity. Here, watermarking transparency and resistance are more important than others. Transparency is the invisibility of the information hidden in an image, and resistance is the resistance of a watermark signal against various image processing techniques and intentional or inadvertent attacks. These two characteristics are in contrast with each other, that means, an increase in either one of them will always cause a decrease in the other. One of the factors effective at creating a balance between transparency and resistance, is the adaptive and optimized selection of watermark strength coefficient. Watermark strength coefficient, represents a watermark's injection into the host image. An increase in this coefficient, increases resistance and decreases transparency, and vice versa. The proposed algorithm in this scheme for intelligent watermarking is based on GA and the HVS. This scheme is an adaptive watermarking method in the area of the discrete cosine transform (DCT) for digital images [2].

II. Genetic Algorithm (GA)

A genetic algorithm (GA) is a method for solving both constrained and unconstrained optimization problems based on a natural selection process that mimics biological evolution. The algorithm repeatedly modifies a population of individual solutions. At each step, the genetic algorithm randomly selects individuals from the current population and uses them as parents to produce the children for the next generation. Over successive generations, the population "evolves" toward an optimal solution. You can apply the genetic algorithm to solve problems that are not well suited for standard optimization algorithms, including problems in which the objective function is discontinuous, no differentiable, stochastic, or highly nonlinear [3].

Before a GA can be run, a suitable coding (or representation) for the problem must be devised. We also require a fitness function, which assigns a figure of merit to each coded solution. During the run, parents must be selected for reproduction, and recombined to generate offspring. The most common way to show chromosomes in genetic algorithms is binary strings. Decision variables are converted to binary form and then after these variables are joined together, a chromosome is created. This method is the most common coding method, but there are also other rapidly developing methods such as representing with real numbers.

Also a fitness function must be devised to assign a value to each coded solution. During the execution, parents are selected for reproduction, and are combined together via mating and mutation operators to produce new children. This process is repeated several times until the next population generation is produced. Next, this population will be investigated and if the convergence criteria are met, this process is ended [4].

III. Intelligent Image Watermarking in the Proposed Scheme

The proposed algorithm in this scheme for intelligent watermarking is based on GA and HVS. This scheme is an adaptive watermarking method in the area of the discrete cosine transform (DCT) for digital images. In this method, the host image is classified into non-overlapping 8×8 blocks and watermark bits are embedded into the DCT coefficients of these blocks. To increase the security of this method, embedding locations are selected randomly. The selected blocks are classified into six different classes based on characteristics such as texture, brightness and proximity to edges. Also, a support vector machine (SVM) is used for the simulation of human visual system (HVS) for the classification of the blocks. One of the factors effective at creating a balance between transparency and resistance, is the adaptive and optimized selection of the watermark strength coefficient. Watermark strength coefficient represents the watermark injection into the host image. An increase in this coefficient, increases image resistance and decreases its transparency, and vice versa. Adaptive watermarking methods which are based on the HVS, determine the watermark strength coefficient in an adaptive way suited for the HVS [5].

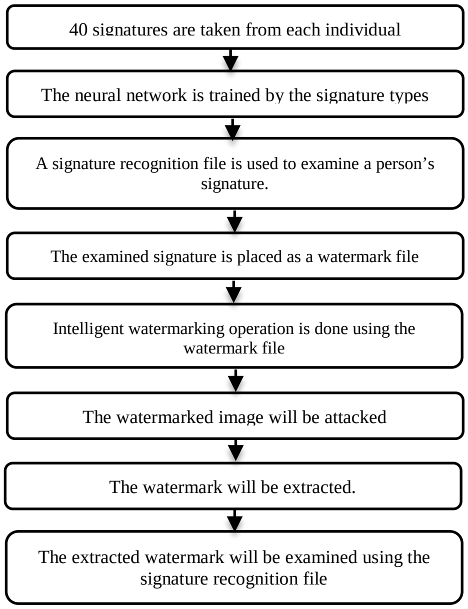

40 signatures are taken from each individual
The neural network is trained by the signature types
A signature recognition file is used to examine a person's signature.
The examined signature is placed as a watermark file
Intelligent watermarking operation is done using the watermark file
The watermarked image will be attacked
The watermark will be extracted.
The extracted watermark will be examined using the signature recognition file

Fig. 1. A Flowchart Of The Overall Process Of The Proposed Scheme

A. Watermark embedding algorithm

The proposed watermark embedding method, is a blind watermarking approach in the area of the DCT. Therefore, watermark extraction does not require the original image. If the host image, is image 'I' with the dimensions of M*N and the watermark image, is a binary image with the dimensions of $*$, to embed the watermark in the host image, first, image 'I' will be classified into non-overlapping 8×8 blocks, and a DCT is taken from each of them. Next, the DCT coefficients of each block, are adjusted in a zigzag form:

$$F_k = DCT\,(I_k) \quad 1 \le k \le k_t \tag{1}$$

F$_k$, includes the DCT coefficients of the k(th) block in host image 'I' which are adjusted in a zigzag form, and kt shows the total number of 8×8 blocks $k_t = \left[\frac{M}{8}\right] \times \left[\frac{N}{8}\right]$. Each DCT block is made of a combination of 64 coefficients. This is shown in figure 2-4.

$F_k(1)$	$F_k(2)$	$F_k(6)$	$F_k(7)$	$F_k(15)$	$F_k(16)$	$F_k(28)$	$F_k(29)$
$F_k(3)$	$F_k(5)$	$F_k(8)$	$F_k(14)$	$F_k(17)$	$F_k(27)$	$F_k(30)$	$F_k(43)$
$F_k(4)$	$F_k(9)$	$F_k(13)$	$F_k(18)$	$F_k(26)$	$F_k(31)$	$F_k(42)$	$F_k(44)$
$F_k(10)$	$F_k(12)$	$F_k(19)$	$F_k(25)$	$F_k(32)$	$F_k(41)$	$F_k(45)$	$F_k(54)$
$F_k(11)$	$F_k(20)$	$F_k(24)$	$F_k(33)$	$F_k(40)$	$F_k(46)$	$F_k(53)$	$F_k(55)$
$F_k(21)$	$F_k(23)$	$F_k(34)$	$F_k(39)$	$F_k(47)$	$F_k(52)$	$F_k(56)$	$F_k(61)$
$F_k(22)$	$F_k(35)$	$F_k(38)$	$F_k(48)$	$F_k(51)$	$F_k(57)$	$F_k(60)$	$F_k(62)$
$F_k(36)$	$F_k(37)$	$F_k(49)$	$F_k(50)$	$F_k(58)$	$F_k(59)$	$F_k(63)$	$F_k(64)$

Fig. 2. DCT coefficients adjustment method

In this proposed method, in order to increase the watermarking security, two keys of key1 and key2 have been used to determine the watermark embedding locations. It is assumed that the number of the watermark bits is lower than the 8×8 blocks in the host image $M_w * N_w \le k_t$. Therefore, utmost one bit of watermark is embedded in each block. First, the DCT blocks are selected by the number of the watermark bits via key1, which are called B$_k$.

$$B_k \subseteq F_k \quad 1 \le k \le M_w * N_w \quad 1 \le k \le k_t \tag{2}$$

Next, via key2, in each selected block, one of the DCT coefficients in the intermediate frequency band will be selected for embedding the watermark bit. For the watermark strength coefficients to be minimized to the location of the DCT coefficients, only coefficients 11 to 15 will be used for this. In each DCT block, coefficients 11 to 15 will be used because we want to consider the minimum watermark strength coefficient for embedding so image transparency will be increased after watermarking. These coefficients are of the intermediate frequency band. The selected coefficient in block B$_k$ will be calledc$_k$. So, $B_k\,(C_k), 1 \le k \le M_w * N_w$, show the watermark embedding location. Now, in order to embed the watermark in the host image, first, we define $\tilde{B}_k\,(i)$ as follows:

$$\tilde{B}_k\,(i) = B_k\,(1) * R\,(i) \quad 1 \le k \le M_w * N_w \tag{3}$$

$\tilde{B}_k\,(i)$ is an approximate of Bk(i) and is used as a reference value for watermark embedding and extraction. Ultimately, watermark embedding per bit is as follows:

$$if \quad w(k) = 0$$

$$B_k(c_k) = \begin{cases} Min(B_k(c_k), \tilde{B}_k(c_k) - \alpha_k) \\ Max(B_k(c_k), \tilde{B}_k(c_k) + \alpha_k) \end{cases} \tag{4}$$

$$if \quad w(k) = 1$$

a_k is watermark strength coefficient in block B_k. After watermark embedding, a DCT reaction is taken from the resulting blocks so image Iw which is the watermark carrying image is obtained [6].

B. Watermark extraction algorithm

If image '$\overset{?}{I}$' with the dimensions of $M^{'} * N^{'}$, is the image carrying the watermark, in order to extract the watermark, first, '$\overset{?}{I}$' will be classified into non-overlapping 8×8 blocks and DCT is taken from each of them. In the next step, using key1, the blocks carrying the watermark ($\overset{?}{B}_k$), and then using key2, the coefficients in which the watermark is embedded ($\overset{?}{c}_k$), will be identified. Finally, watermark bits $\overset{?}{w}$ will be extracted from each of the blocks carrying the watermark, which is shown below:

$$W^{'}(k) = \begin{cases} 1 & if \ B^{'}_k(c^{'}_k) \geq \tilde{B}_k(c^{'}_k) \\ 0 & els \end{cases} \tag{5}$$

C. Determining watermark strength coefficient

At this stage, the watermark strength coefficient will be adaptively determined. The adaptive determination of this coefficient, includes three stages:

- Extracting appropriate characteristics from the image blocks based on HVS characteristics.

- Categorizing the blocks into different classes based on the extracted characteristics.

- Determining the watermark strength coefficient for each class [5].

D. HVS-based characteristics extraction

Watermark embedding into a host image is actually the task of adding a weak noise to a strong signal, and as long as the noise power is below the just noticeable difference 1 (JND), the human eye cannot detect it. Studies have shown that the human eye is as follows:

- It has lower noise sensitivity in higher resolution groups.

- It has lower noise sensitivity in areas of an image with higher or lower brightness.

- It has lower noise sensitivity in areas with high texture, however, it has higher sensitivity to the proximity of edges.

Based on this, in a watermarking system, it is possible to consider different watermark strength coefficients for different areas of an image. For example, in noisy textures, a higher watermark strength coefficient can be used around the edges and in bright or dark areas. In this scheme, different image blocks are classified into six classes based on texture and brightness, and different watermark strength coefficients are determined for each class. The six classes are as follows:

T1: blocks with a smooth texture and high brightness

T2: blocks with a smooth texture and average brightness

T3: blocks with a smooth texture and low brightness

T4: blocks with edges

T5: blocks with a relatively noisy texture (coarse texture)

T6: blocks with a very noisy texture (fine texture)

In this scheme, four characteristics are used to classify the blocks into the aforementioned classes: brightness level, entropy, variance and contrast. In other words, the four characteristics are extracted from each block, then based on them, the class corresponding to each block is determined. The brightness level of each block is obtained by averaging from its pixel values. When the brightness of a block is low or high, it is possible to use a higher watermark strength coefficient. Second moment or variance has a especial importance in texture description and is a criterion of intensity contrast which can be used to determine the relative smoothness of images. Entropy is a criterion which shows dispersion in pixels intensity. Thus, in images having a texture, it has higher values. Brightness level, variance and entropy are obtained from the equations below:

$$\mathrm{Mean} = \sum_{i=0}^{l-1} \left(z_i P(z_i)\right) \tag{6}$$

$$\mathrm{Var} = \sum_{i=0}^{l-1} \left((z_i - \mathrm{Mean})^2 P(z_i)\right) \tag{7}$$

$$\mathrm{Ent} = -\sum_{i=0}^{l-1} (P(z_i) \log_2 P(z_i)) \tag{8}$$

In these equations, z_i represents brightness and l shows the number of gray levels. $P(z_i)$ represents the probability of brightness intensity z_i of an image, and equals the ratio of the number of pixels with brightness z_i to total image pixels. Texture criteria which are only calculated using a histogram, like the above criteria, do not carry any information about the relative location of pixels relative to each other. This point is important when describing a texture, and a method for embedding this type of information in a texture analysis process is to consider the relative location of each pixel. For this purpose, in this scheme, a second order elemental differential moment or in other words, a contrast criterion is used. For this purpose, first, a co-occurrence matrix is formed for the image block. A co-occurrence matrix is a matrix whose elements show the number of times when the pixel pairs of z_i and z_j are placed in a particular position relative to each other. Here, each of the elements of this matrix (g_{ij}), shows the number of times when the pixel pairs of z_i and z_j are placed next to each other in each other's eightfold neighborhood. The contrast criterion for each image block is calculated as follows:

$$Cont = \sum_{i=0}^{l-1} \sum_{j=0}^{l-1} ((z_i - z_j)^2)(P(z_i - z_j)) \tag{9}$$

z_i and z_j represent brightness intensity and $P(z_i, z_j)$ is the probability of them being placed next to each other which is calculated as follows:

$$\mathrm{P}(\mathrm{z_i}, \mathrm{z_j}) = (\mathrm{g_{ij}}/\mathrm{n}) \qquad (10)$$

n represents the total number of pixel pairs placed next to each other, and in other words, equals the sum of the co-occurrence matrix elements. As is clear from equation (10), if the difference in the brightness intensity of adjacent pixels is higher, the contrast will be higher. Variance, entropy and contrast are used to determine block texture. When entropy and variance have small values, the image is smooth. If entropy is high, if variance has a large value, it is edge or otherwise texture. In images with a very noisy texture (fine texture), contrast has large values [7].

E. Classification of blocks via SVM

In order to determine watermark strength coefficients α_k in embedding blocks B_k, the 4 characteristics of brightness level, variance, entropy and contrast are extracted, next, based on them, the blocks are classified into six classes. In this scheme, for block classification, a trained support vector machine (SVM) is used [8]. In previous papers where block classification has been used to make watermarking adaptive [6], mostly, classic classification methods based on thresholding for extracted characteristics are used. Such classifier will not provide the necessary accuracy, because the HVS is an entirely complicated and nonlinear system. Therefore, here, an SVM is used to find a relationship between the mentioned characteristics and their corresponding classes because of its high capability at simulating the HVS and its high capabilities at learning, nonlinear generalization and approximation. To use SVM in data classification, first, it must be trained. For this purpose, in this scheme, 1000 image blocks with different texture and brightness are used as training samples. At the end, the trained SVM will be used to determine the class of the B_k blocks.

$$\text{Class } (B_k) = \text{SVM } (mean_k, var_k, ent_k, cont_k) \qquad (11)$$

$$Class\,(B_k) \in \{t1, t2, t3, t4, t5, t6\} \qquad (12)$$

SVM, represents the process of data classification via the SVM. Since the number of the classes is more than 2, the one-against-one method is used for data classification $(\mathrm{mean_k}, \mathrm{var_k}, \mathrm{ent_k}, \mathrm{cont_k})$. The characteristic vector is extracted from block $\mathrm{B_k}$ which includes brightness level, variance, entropy, and contrast [9].

F. Determining watermark strength coefficients via a GA

After classifying the blocks into the six mentioned classes, the suitable watermark strength coefficient for each class is determined using a GA. We define vector S as below which shows the watermark strength coefficient in each class.

$$S = [s1,s2,s3,s4,s5,s6] \qquad (13)$$

si represents the watermark strength coefficient in the blocks of $\mathrm{t_i}$ class $S_i = S(t_i)$ The objective is to find the optimal S via the GA. If S^* is the vector resulting from the GA, the values of α_k in the section of watermark embedding are obtained from the equation below:

$$\alpha_k = S^*(Class\,(B_k)) \qquad (14)$$

The GA starts with a primary population of S vectors. For every S vector in the population, the resulting fit functions of a number of them are selected as the parents. After carrying out crossover and mutation operations on the parents and production of children, a new generation including a new population of S vectors will be formed. This process continues until the population is converted into an optimal vector. At the end, the vector with the greatest fit value in the last generation, will be the ultimate response of the algorithm (S*). In order to define the fit function, the watermarking transparency and watermark's resistance will be calculated for every S vector. Therefore, for every S vector, a watermark embedding operation is carried out. Next, in order to evaluate the watermarking transparency, the similarity level of the watermarked image to the host image will be measured. Now the simplest and most useful criteria for measuring similarity are MSE and PSNR which are calculated from the equations below and the reason for it is the simple calculation and inclusion of an understandable physical meaning.

$$MSE = (1/M*N)\sum_{i=1}^{M}((I(i,j) - I'(i,j))^2 \qquad (15)$$

$$\mathrm{PSNR{=}10{*}log10((255{\hat{}}2)/MSE)} \qquad (16)$$

After evaluating the watermarking transparency level through the calculation of the structural similarity index between the host image and the watermarked image, for evaluating the watermark resistance level, a number of attacks and image processing operations are carried out on the watermarked image. Then the watermark is extracted from the images, and the BCR index for each of them, between the original watermark and the extracted watermark is calculated.

$$BCR(w, w^2) = (\sum_{i=1}^{M_w}\sum_{j=1}^{N_w} XOR(w(i,j), w'(i,j)) \qquad (17)$$

The maximum value for BCR is 1, and this value is obtained only if the original watermark and the extracted watermark are the same. The fit function for each S vector is defined as below:

$$F(s) = PSNR(I, I') + 1/p\sum_{k=1}^{p} BCR_k(w, w') \qquad (18)$$

'I' is the host image and I' is the watermarked image which was obtained via the separation of the watermark in image 'I' through the use of an S vector. P shows the number of attacks applied to image I'. W is the original watermark and w' is the watermark extracted from each of the attacked images. In this scheme, two attacks including a median filtering and a JPEG compression with a quality factor of 40 for evaluation of the watermark resistance level in the fit function [14] were used.

IV. Signature Recognition in the Proposed Scheme

The main difference between simple watermarking and handwritten signature-based watermarking is that in simple watermarking, an ordinary logo is placed behind the host image but in handwritten signature-based watermarking, a person's handwritten signature is used as the watermark. In the proposed scheme, signature recognition is done based on static signature characteristics. The purpose in this project, was network training for three people, which, 40 handwritten signatures of every user have been taken and scanned. Next, the waste areas around the signature are removed. For this purpose, after acquiring the image size, the sum of the elements of its rows and columns is calculated and finally, a figure is shown from an area whose sum of row and column is lower than the row and column of the image, because the background of the signatures was white and they are considered as being monochrome and the signatures were black and zero. We place the cut image in that same primary matrix and then alter its size and change it into a 70 × 20 matrix. Now, we change the figure matrix into a column shaped one and change it into a 1400 × 1 matrix. Now using a Perceptron Neural Network with 3 nerves and with a target vector as [100,010,001] which represent the first, second and third person, respectively, these signatures are trained to the network. The interesting point is that the watermark acceptable for the host image in the watermarking in the proposed scheme, must be of a 70 × 20 size. Also, since the person's signature may be written in different colors, before the network training, the signatures are changed from the RGM mode into binary mode, so the watermark image finds a 0 and 1 mode. Therefore, during the network training, the signatures are primarily changed into the considered size and are given gray color and then will be trained to the network.

After the network is trained, one sample of a person's handwritten signature will be changed into the mentioned size and color and is hidden behind the host image as the watermark. After that, this watermark can be extracted before or after the attacks, and the signature's originality can be verified using the trained network, and it will be possible to verify whose signature it is. The flowchart of the process of network training for handwritten signatures is shown in figure (3). The interesting point about watermarks is that, given that a watermark is a person's handwritten signature, after it is altered to the size acceptable for watermarks that is 70 × 20, only a part of the signature is selected and used as a watermark. An example of this is shown in figure 6.

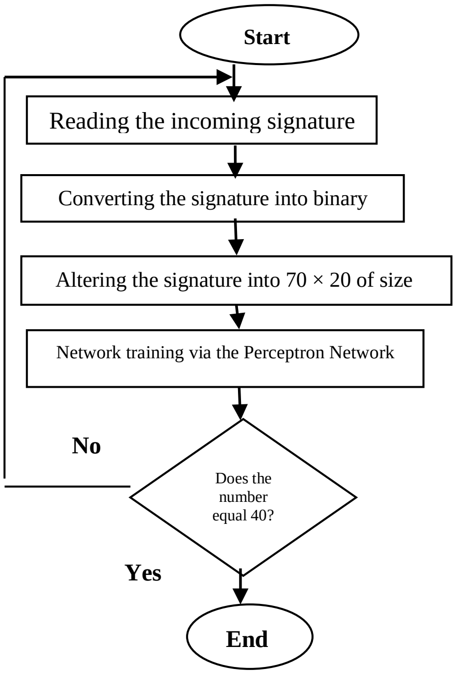

Start
Reading the incoming signature
Converting the signature into binary
Altering the signature into 70 × 20 of size
Network training via the Perceptron Network
No
Does the number equal 40?
Yes
End

Fig. 3. flowchart of the signature recognition network training process

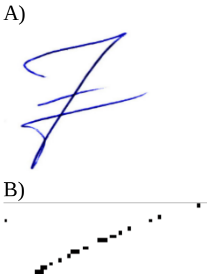


Fig. 4. A) original handwritten signature, B) signature prepared as the warmark

V. SVD Statistical Method

Recently, Singular Values Decomposition (SVD) in watermarking has become very popular due to the matrix characteristics in its attractive mathematics. SVD is one of the useful tools in Linear Algebra with various uses in image compression, watermarking and other signal processing areas. The main idea of this method is that the SVD of the cover image is calculated and then special values are modified for watermark embedding. If 'A' is an NXN matrix, after that, the SVD of this matrix can be defined as follows:

BCR watermark correctness in SVD	BCR watermark correctness in GA	Image	attack
0.50	0.96	Peppers	JPEG40
0.53	0.95	Mandril	
0.49	0.98	Cameraman	
0.61	0.98	Lena	Median filtering
0.65	0.97	Mandril	
0.62	0.98	Cameraman	

$$A=U*S*V^T \tag{19}$$

In this equation, U and V are orthogonal matrixes and S is a diagonal matrix. The diagonal elements of matrix S, are special values and follow the characteristic below:

$$S\ (1, 1) > S\ (2, 2) > S\ (3, 3) > \ldots\ldots\ldots.. > S\ (n, n) \tag{20}$$

The SVD-based watermarking scheme is provided by Kumar Gupta et al. (2010), this method is a combination of watermarking in the area of DWT and SVD. DWT, decomposes an image into four frequency groups: LL, HL, LH and HH. LL represents low frequency, HL and LH represent average frequency and HH represents high frequency. LL shows approximate details, HL shows horizontal details, LH provides vertical details and HH highlights the diagonal details of an image. In this suggestion, the HH group is selected for watermark embedding, because it includes more accurate details and provides a small contribution to image energy. Therefore, watermark embedding does not affect the image perceptual correctness [10]. The proposed scheme is based on an idea of replacing special values from the HH group with special values from the watermark. The special values of the HH group of various experimental images, have shown that these values are between 84 and 173. If a watermark is selected in a way whose special values are placed inside the given range, after that, the energy of the special values of the watermark will almost equal the special values of the HH group. For this purpose, the replacement of special values does not affect the perceptual image quality and the energy level of the HH group. In this method, the size of the host image, was considered as 512 × 512 and the watermark size was considered as 256 × 256, which during the process of watermarking, the size of the watermark changes and becomes equal with the size of the HH group.

VI. Results of Implementation of the Proposed Intelligent Scheme and Comparing It with the SVD Method

Based on the results of Gupta et al. (2010) which investigated the resistance and transparency of watermarked images via the SVD method, we will compare this method with the proposed method. In terms of image resistance and transparency, the GA method is better than the special values method. Experiments were performed on Bubble, Lena and Cameraman images. In table (1), the image transparency level in the two methods after watermarking is shown, and in table (2), image resistance to attacks is shown. The attacks tested in both methods include JPEG40 compression attacks and median filtering [10].

TABLE I. Image Transparency After Watermark Embedding

PSNR transparency in SVD	PSNR transparency in GA	Image
43.33	68.98	Peppers
50.67	64.74	Mandril
47.42	68.57	Cameraman

TABLE I. watermark correctness level after various attacks

As is seen in table 1, image transparency in the GA method is more than the SVD statistical method. Also, based on the results in table 2, we will see that the correctness level of the watermark after various attacks, is better in the GA method than the SVD method. The reason for the superiority of the intelligent making GA scheme compared to the SVD statistical method at image transparency is that in the GA method, the watermark strength coefficients for embedding are considered as the smallest values possible, and smaller bits of the host image are placed for covering the watermark. For example, in the following, we will investigate the Cameraman image before and after watermarking and after the attacks in the intelligent method.

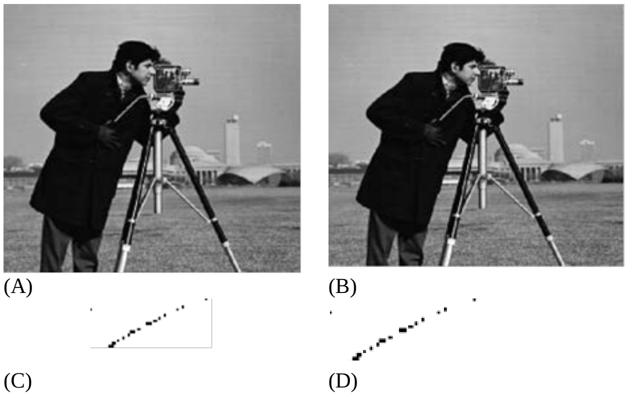
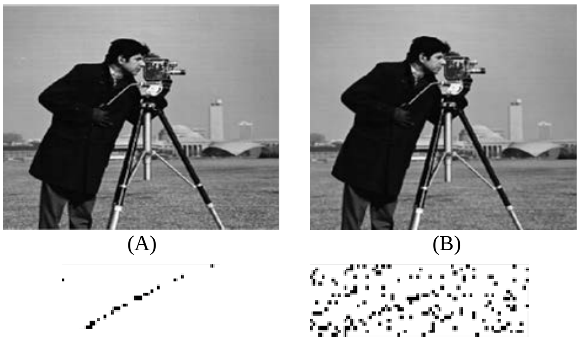


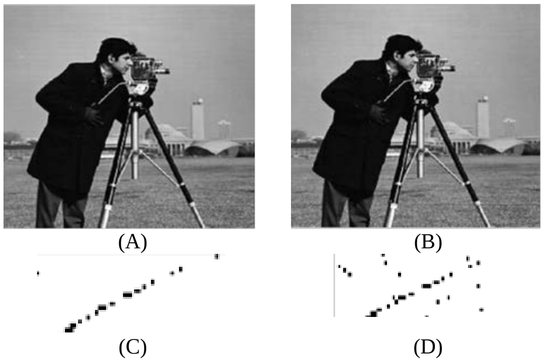
Fig. 5. A) main image, B) watermarked image, C) main watermark, D) extracted watermark



(A) (B)

(C) (D)

Fig. 6. A) watermarked image, B) image after median attack, C) watermark extracted before the attack, D) watermark extracted before median attack



(A) (B)

(C) (D)

Fig. 7. A) watermarked image, B) image after a JPEG40 attack, C) watermark extracted before the attack, D) watermark extracted before a JPEG40 attack

VII. Conclusion

Biometrics are the most secure identity verification factors in the world of information and communication, which also provide improved accuracy, speed, ease and reduce costs. Here, authentication via a person's signature is one of the most widely used authentication methods and it is because of its importance in e-commerce security issues where the real identity of the person who signs documents is discovered. Watermarking is the act of hiding a data (watermark) in a covering data (cover) in order to exercise of the right of ownership on the cover. The difference between a normal watermarking and a handwritten signature-based watermarking is that in normal watermarking, one image with one sign is selected and used as the watermark, but in the method of handwritten signature-based watermarking, the person's signature is embedded in the image and prevents all attempts to copy it.

In images which are watermarked, the two topics of resistance to attacks (or any changes) and quality are important. The balance between resistance and quality can be properly achieved through the adjustment of the embedded parameters. In intelligent watermarking, evolutionary computing algorithms such as genetic algorithms and particle swarm optimization, automatically find the embedded parameters which are the results of optimization for each image. For intelligent watermarking, techniques such as fuzzy logic, genetic algorithms and artificial neural networks are used.

In the proposed scheme, a GA is used for intelligent watermarking. Watermark embedding in this scheme, was performed based on the DCT method and in an adaptive way and the results from implementing it compared to the results of the SVD statistical method, provided better transparency and resistance for the image. Signature recognition in the proposed scheme was performed via the perceptron neural network and given the static characteristics of the signature, the network was trained and it was tested. Since the person's signature was considered as the watermark, despite the addition of many noises after the attack to the watermark image, still, the signature recognition was properly done and the signatures of all the individuals were recognized without any mistakes. Based on what is mentioned above, handwritten signature-based intelligent watermarking will be a method that provides more security in authentication systems and copyright issues and is done with optimal quality and resistance.

VIII. Recommendations for Future Research

In the future, the three items below can be applied to the proposed scheme to improve it:

1) In signature recognition, for more accurate recognition, instead of the static characteristics of a signature, its dynamic characteristics can be used.

2) The proposed method for handwritten signature-based intelligent watermarking can be tested with more attacks and its results can be investigated.

3) The present scheme was implemented on black and white images, and to further develop it, it can be used on black and white images as well.

References

[1] Z. Toni, providing an optimal method for image hiding using a learning algorithm, (Master's thesis), Sharif University of Technology, Iran.2010.

[2] E. Vellasques, R. Sabourin,E. Granger, A high throughput system for intelligent watermarking of bi-tonal images.Applied Soft Computing, vol. 11, no. 8, pp. 5215-5229, 2011.

[3] D.E. Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning", Addison-Wesley, 1989.

[4] J.H. Holland, "Adaptation in Natural and Artificial Systems", The University of Michigan Press, Ann Arbor, MI, 1975.

[5] P. Nafisifard, Darhami, A. M. Latif, Adaptive watermarking of digital images based on machine learning. Intelligent Systems in Electrical Engineering, vol. 2, no. 4, pp. 47-64, 2011.

[6] Z. Lu, S. Jiang and H. Dong, "Adaptivewatermarking algorithm based on humanvisual system", Journal of harbin institute oftechnology, vol. 35, no. 2, pp. 138–141, 2003.

[7] R. C. Gonzalez and R. E. Woods, "Digitalimage processing, 3rd Ed", PrenticeHal. 2008.

[8] J. Huang, Y. Q. Shi and R. Yao, "Adaptiveimage watermarking based on blockclassification", Journal of image andgraphics, vol. 4, no. 8, pp. 640–643, 1999.

[9] F. Meng, H. Peng, Z. Pei, and J. Wang, "A Novel Blind Image Watermarking Scheme Based on Support Vector Machine in DCT Domain", IEEE International Conference on, Computational Intelligence and Security,2008.

[10] A. Kumar Gupta, SM. Raval, A robust and secure watermarking scheme based on singular values replacement. Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar 382 007, India, vol. 37, no. 4, pp. 425-440, 2010.