International Journal of Innovative Computing, Information and Control
Volume **8**, Number **2**, February **2012**

 ISSN 1349-4198
pp. 1205–1220

DIGITAL IMAGE WATERMARKING BASED ON PARAMETERS AMELIORATION OF PARAMETRIC SLANT-HADAMARD TRANSFORM USING GENETIC ALGORITHM

Alimohammad Latif[1] and Ahmad Reza Naghsh-Nilchi[2]

[1]Department of Electrical and Computer Engineering
Yazd University
Yazd, Iran
alatif@ yazdui.ac.ir

[2]Department of Computer Engineering
Faculty of Engineering
University of Isfahan
Isfahan, 81746, Iran
nilchi @ eng.ui.ac.ir

Received June 2010; revised November 2010

Abstract. *In this paper, digital image watermarking based on parameters amelioration of parametric slant-Hadamard transform using genetic algorithm is presented. In image watermarking procedure, the image is divided into separate blocks and the parametric slant-Hadamard transform is applied on each block individually. Then, the watermark is embedded in the transform domain and the inverse transform is carried out. The main advantage of the selecting parametric slant-Hadamard transform is the availability of transform parameters which could be used to ameliorate the fidelity and robustness. In general, the fidelity and robustness properties of watermarking schemes are in conflict. Here, a genetic algorithm is introduced to ameliorate the transform parameters to improve both the fidelity and robustness simultaneously. Additionally, to increase the security of our algorithm, different sets of parameters are sought for each block individually. Experimental results show that the introduced watermarking scheme produces remarkably high fidelity with highly robust watermark against various attacks.*
Keywords: Digital image watermarking, Genetic algorithm, Parametric slant-Hadamard transform, Fidelity, Robustness

1. **Introduction.** Easy access to digital images via the Internet and other communication means as well as the availability of powerful software and hardware tools to edit digital images have made authentication of digital images a problematic issue. An effective solution to resolve this issue is through digital image watermarking techniques. Digital image watermarking is a technique of embedding additional information called watermark into an image by preserving perceptual quality of the original image. The watermark may be detected or extracted for owner identification and/or integrity verification of the watermarked images [1].

There are two types of watermarked images: visible or invisible. The visible watermarked images consist of a visible message or a company logo indicating the ownership of the image. While, the invisible watermarked images are almost identical to the original ones though the embedded watermarks and they are invisible to normal eyes [2]. In this article, we consider the invisible watermarked images.

Among others, invisible digital image watermarking algorithms need to satisfy two very important requirements: fidelity and robustness. The fidelity makes sure that the

distortion between the original and watermarked image remains imperceptible to a human observer. While the robustness ensures the ability of the authorized party to extract the watermark, with an acceptable quality, from an attacked watermarked image [3].

The watermarking algorithms are classified depending on how the watermark is embedded. In fact, depending on the domain in which the watermark is embedded, digital watermarking techniques can be classified as spatial and spectral domain techniques. In the spatial domain methods, a watermark is inserted into an image by modifying the images' pixel values directly [4]. However, spectral domain approaches transform the original image into the frequency domain and modulate the transfer's coefficients to embed the watermar. In general, spectral domain methods are more robust than spatial domain against many common attacks [5].

A fundamental advantage of transform-based techniques is that the transformed version of the image has good energy compactness properties and most of image energy can be captured within a relatively small number of the transform coefficients. It is to be noted that the transform basis functions corresponding to these coefficients carry the most perceptually important information of the image. Also, transform-based domain watermarking techniques facilitate the process of selecting the most suitable portions of the original image to insert a robust and invisible watermark [6].

Maybe, the earliest transforms which were utilized in watermarking schemes were Discrete Fourier Transform (DFT) [7]. This transform scheme could utilize rotation, scale and translation invariant properties. Later, Pun embedded the watermark in the DFT coefficients with the highest magnitudes and used the similarity measure in detection procedure [8].

Next, Discrete Cosine Transform (DCT) was extensively utilized in watermarking schemes. By using the DCT, an image was divided into frequency bands, and the watermark was embedded in low and middle frequency bands. Sensitivities of the Human Visual System (HVS) to changes in these bands were studied in the context of JPEG compression, and the results of these studies were exploited to minimize the visual impact of the watermark embedding distortion [9].

In addition, many multi-resolution watermarking techniques were proposed by using Discrete Wavelet Transform (DWT). In this group of watermarking schemes, the original image and watermark were decomposed into sub-bands and then, the watermark sequence was embedded into the corresponding level of the transformed image. The sub-band decomposition technique facilitated placement of the watermark which exploited HVS characteristics to obtain more fidelity of the watermarked images [10].

Among other transform-based schemes, Discrete Hadamard Transform (DHT) and its variants were used extensively to develop some effective image watermarking algorithms [11]. One of noticeable methods is a work done by Li et al. They proposed a block-based DHT method where watermark information was inserted into Hadamard coefficients. The DHT domain watermarking method shows some advantages over other transform-based methods including low computation cost and robust watermark. The robustness was due to the sequencing effect which packed energy of the image in the low and middle frequency coefficients [12].

Another transform-based method which was usually used for semi-fragile digital image watermarking, required for image authentication and self-restoration, was Slant Transform (ST). Zhao et al. embedded the watermark bits into the middle frequency region of each block after applying the ST to the original image. Then, the original image was compressed and the watermark was embedded into the least significant bits of the watermarked image for subsequent self-restoration. They indicated that the ST was more

robust, accurate and faster than other transforms such as the DCT and pinned sine transform [13].

It is well known that the ST is the best compaction performance among the non-sinusoidal fast orthogonal transforms but it is not comparable in its compaction performance measure among the sinusoidal transforms such as the DCT [14]. Note that, in general, there is a trade off between the compaction performance of an orthogonal transform and its computational complexity. For example, the Karhunen-Loeve Transform (KLT) is an optimal transform in compaction but definitely not low in computational complexity [15]. Therefore, the need arises for the ST improvement schemes without incurring their computational complexity.

To improve the performance of the ST, Agaian et al. introduced a new concept for a class of parametric slant transform that includes special cases of the slant and Hadamard transforms. Their work led into the Parametric Slant-Hadamard Transform (PSHT) with different applications [14].

A remarkable property of the PSHT is that it is guaranteed to have $2^{n-1}-1$ zero coefficients for a transform of order 2^n. In particular, for digital image applications, an image is transformed to a domain in which many coefficients are zeros; i.e., energy in the transform domain is less distributed. Also, the entropy of the coefficients in the PSHT domain decreases compared with other domains that do not have such energy compactness. Furthermore, the PSHT matrices are the product of sparse matrices, so there are fast algorithms to compute the transform. The PSHT can also be implemented with inexpensive hardware because all the transform operations require only shifters and adders rather than multipliers. Additionally, in the most transform-based algorithms, the size of the transform matrix is an integer power of two; however, in the PSHT, the size of matrix is power of an arbitrary number [16].

The motivation behind using the PSHT as the basis for embedding a watermark into an image in this work is that the parameters in this transform proved to be suitable for controlling the fidelity and robustness of watermarking scheme. It is important to note that if these parameters are being changed in the embedding process, the requirements of watermarking would change, but does not hurt the watermark extraction; however, if these parameters are changed, even slightly, in the extracting process, the watermark cannot be extracted properly. As a result, the proper amelioration of these parameters to lead the required fidelity and robustness in the watermarking process becomes an important task. In addition, the sensitiveness of the extracting process to any slight changes to these parameters may well be used as encryption keys for watermarking authorization [17].

The history of taking advantage of the proper selection of parameters in PSHT goes back to a work done by Nassiri et al. in digital images processing for a texture feature extraction application. They showed that a subtly parameter modification of the PSHT could outperform from the ordinary Walsh-Hadamard transform to discrete cosine transform for their feature extraction application. In fact, by changing the transform parameters and selecting some suitable parameters, they could achieve better feature extraction for different images [18].

In addition, the PSHT is also used for digital image watermarking in the past by Xie et al. In their method, they partitioned the host image into non-overlap blocks and used a class of adaptive parametric slant bases for each block. They applied spectral spectrum technique for watermarking embedding procedure. They utilized the average correlation between the extracted watermark and original watermark based on blind extraction algorithm in the watermarking detection procedure. They showed that their method's robustness performance was comparable with the other orthogonal domain watermarking approaches with the presence of lossy compression. Their results indicated that the PSHT

watermarking scheme had better performance consistently across all compression levels, for both signals that were rich in low frequency and high frequency components [19]. Xie pointed out an algorithm to select the transform parameters against only the JPEG compression attack and they did not take advantage of the PSHT parameters in their scheme as the one is proposed in this paper.

On the other side, Genetic Algorithm (GA) has been used in digital image processing applications including image watermarking. In the past, researchers utilized the evolutionary computation strategy to acquire nearly optimal parameters in digital image watermarking to improve the performance of their schemes. As an example, Huang et al. explored the optimal watermark embedding position by the GA, to improve the quality of protected images sufficiently [20]. In addition, Shih et al. proposed a method which embedded the watermark into the frequency domain. In the watermarking schemes where the watermarks were embedded into the least significant bit of the coefficients, there occurred the rounding errors. They used the GA to reduce the rounding error effects and enhanced the fidelity and robustness of the scheme simultaneously [21]. Another example is the work done by Aslantas et al. who explored an optimal watermarking scheme based on singular value decomposition by using the GA. The singular values of the original image were modified by multiple scaling factors to embed the watermark image. Modifications were enhanced by using the GA to obtain a higher robustness without losing much of the image's fidelity [22]. Besides, Kumsawat et al. utilized the GA in an embedding technique that was based on the quantization index modulation technique using digital wavelet domain. They developed an optimization technique using the GA to search for improved quantization step which could enhance the quality of watermarked image and the robustness of the watermark against variety of attacks [23].

Achieving optimal values for the PSHT parameters in the watermarking procedure with closed form solution is proved to be difficult. It is because of the highly nonlinear behavior of the parameters as well as the involved high computational complexity due to the building the required transform matrices. In the past, Xie tackled this problem by introducing an algorithm which approximates polynomial of squared error curve to ameliorate the PSHT transform parameters which could only address the JPEG compression attack [24].

In this study, the very same problem is addressed but a much more powerful solution based on GA is offered. The GA helps us to obtain the solutions with a proper fitness function in the watermarking system. The primary novelty of this study resides in the way a GA-based scheme is exploited in order to search for the parameters that are both able to improve the robustness of the watermark against some attacks (not just JPEG compression attack) and keep the fidelity of the watermarked image high, simultaneously. In other words, since the PSHT outperforms from ordinary Walsh-Hadamard transform to discrete cosine transform, we used this transform that the GA ameliorates the transform parameters for selecting the most suitable transform for each block individually. Furthermore, because the level of the required robustness and the fidelity in different watermarking application may differ, the utilized GA technique for transform parameters selection may be used to obtain the most suitable parameter values that satisfy each certain application requirements, separately.

The rest of this article is organized as follows: in Section 2, the methods including the PSHT, genetic algorithm and watermarking procedure are reviewed; GA-based parameter amelioration is described in Section 3; Section 4 is dedicated to the presenting of the simulation results; in addition, the performance of watermarking against some common attacks is evaluated; finally, the conclusion remarks are presented in Section 5.

2. Methodology.

2.1. Parametric slant-Hadamard transform. In this section, a brief overview of the PSHT representation of image data that employed in watermarking scheme is presented. Let f represents the original image and F the transformed image, the two-dimensional PSHT is given by:

$$F = S_{2^n}.f.S_{2^n}^T \tag{1}$$

where S_{2^n} represents a $2^n \times 2^n$ parametric slant-Hadamard matrix with real values with size of original image, n is an integer number and T denotes the transpose. The inverse transform to recover f from the transformed components matrix, F, is given by:

$$f = S_{2^n}^T.F.S_{2^n} \tag{2}$$

The parametric slant-Hadamard matrix of order 2^n is generated in terms of matrix of order 2^{n-1} using Kronecker product operator [25], denoted by $\bigotimes$, as:

$$S_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3}$$

$$S_{2^n} = \frac{1}{\sqrt{2}} Q_{2^n} (I_2 \bigotimes S_{2^{n-1}}) \quad n > 1 \tag{4}$$

where I_2 denotes the identity matrix of order 2 and Q_{2^n} is the recursion kernel matrix defined as:

$$Q_{2^n} = \begin{pmatrix} \begin{matrix} 1 & 0 \\ a_{2^n} & b_{2^n} \end{matrix} & \vdots & 0_{2^{n-1}-2} & \vdots & \begin{matrix} 1 & 0 \\ -a_{2^n} & b_{2^n} \end{matrix} & \vdots & 0_{2^{n-1}-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} & \vdots & 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \begin{matrix} 0 & 1 \\ -b_{2^n} & a_{2^n} \end{matrix} & \vdots & 0_{2^{n-1}-2} & \vdots & \begin{matrix} 0 & -1 \\ b_{2^n} & a_{2^n} \end{matrix} & \vdots & 0_{2^{n-1}-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} & \vdots & 0_{2^{n-1}-2} & \vdots & -I_{2^{n-1}-2} \end{pmatrix} \tag{5}$$

where 0_M denotes an $M \times M$ zero matrix and I_M represents identity matrix of order M. The parameters a_{2^n} and b_{2^n} are obtained recursively by [26]:

$$a_{2^n} = \sqrt{\frac{3(2^{2n-2})}{4(2^{2n-2}) - \beta_{2^n}}} \qquad b_{2^n} = \sqrt{\frac{2^{2n-2} - \beta_{2^n}}{4(2^{2n-2}) - \beta_{2^n}}} \tag{6}$$

Based on the definition of the PSHT matrix, a parameterized slant matrix is a function of parameters a_{2^n}, b_{2^n} which in turn is a function of sequence of β_i $\{i = 4, 8, \ldots\}$. Note that the user needs to select these transform parameters for his or her application. In this study, the building block of the transformed image is based on the sub-block and the size of the PSHT matrix is 8. Therefore, the elements of this matrix is a function of β_4 and β_8. In our algorithm, we use the GA to suggest the proper values for these parameters in order to ameliorate the fidelity and robustness of the watermarking scheme. Additionally, to increase the security of our algorithm different sets of parameters are sought for each block individually.

2.2. **Genetic algorithm.** Conventional search techniques are often incapable of optimizing non-linear functions with multiple variables. The genetic algorithm methodology, which was first introduced by Holland has become a popular evolutionary optimization algorithm for such problems [27]. This algorithm finds the global optimal solution in complex multidimensional search spaces. The GA is based on the theory of genetics and natural selection. According to this theory, initial population is manipulated into new population over several generations which gradually improve their fitness.

A flowchart of a simple GA is shown in Figure 1 [28]. According to this flow chart, the GA consists of components including random number generator, fitness evaluation, reproduction, crossover and mutation modules.

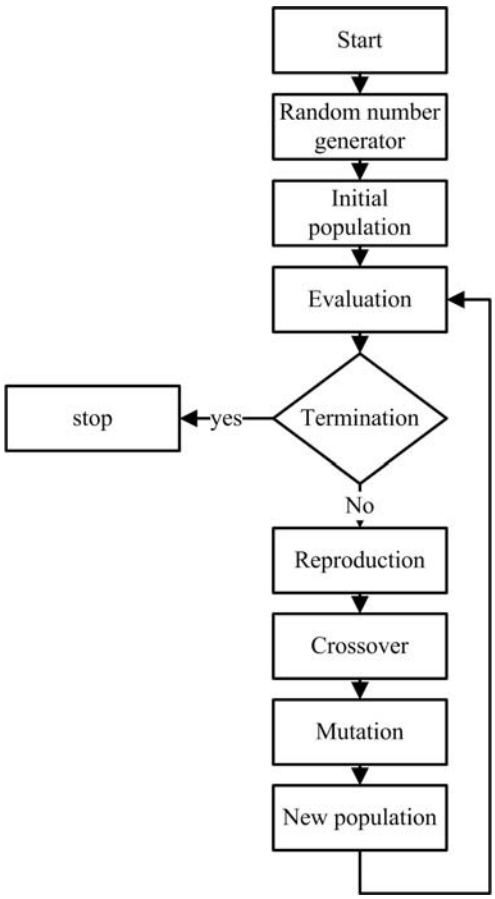

FIGURE 1. Flowchart of a simple genetic algorithm

The initial population needed to be assigned in this algorithm is a set of strings which represents the solutions to a given problem. These strings are generated by the random number generator module and then are encoded into the chromosomes. Associated with each chromosome, a fitness value is computed by the evaluation unit. A fitness value is a measure of the goodness of the solution that it represents. The fitter chromosome has the greater chance to survive during the process [29].

In the initial population, a particular group of chromosomes are chosen as the parents of the following new generation. The new chromosomes are generated from these parents by using genetic operations. These operations include reproduction, crossover and mutation. The aim of the genetic operators is to transform the set of chromosomes into another set with higher fitness values.

Note that the crossover operator chooses pair of chromosomes randomly and produces a new pair. The simplest crossover operation is to cut the original parent chromosomes at a randomly selected point and exchange their tails. The number of crossover operation is governed by a crossover probability. Also, the mutation operator randomly mutates or reverses the values of bits in a chromosome. The number of mutation operation is determined by a mutation rate.

Finally, the GA proceeds with this process and repeats until it meets the terminating condition. The population with the highest fitness value in the final iteration is assumed to be the optimized solution.

2.3. **Watermarking procedure.** Any watermarking scheme consists of embedding and extracting procedures. The former is embedding the watermark in the original image and the latter is extracting the watermark from the watermarked image. In this study, at the embedding procedure stage, the original image is divided into non-overlapped blocks (compatible with the JPEG compression) and then, the PSHT of each block is computed. Afterwards, the middle frequency band of each block is modulated using the following equation [30]:

$$F_W = F + k.W \tag{7}$$

where F is the transformed image, k is the watermark strength, W is the transformed watermark, and F_W is the transformation of the watermarked image. Finally, the inverse PSHT is computed and the watermarked image is obtained.

Our watermark extracting procedure is based on the reverse computation of Equation (7). The reverse equation is:

$$W = \frac{1}{k}(F_W - F) \tag{8}$$

The embedding and extracting procedure of watermarking algorithm is summarized in Tables 1 and 2, respectively.

TABLE 1. Summary of embedding procedure

1. Divide the original image into non-overlapped blocks;
2. Compute the PSHT of each block (GA is used to ameliorate the PSHT parameters);
3. Embed the watermark on the middle frequency coefficients;
4. Compute the inverse PSHT of the result to obtain the watermarked image.

TABLE 2. Summary of extracting procedure

1. Divide the original and watermarked image into non-overlapped blocks;
2. Compute the PSHT of each block;
3. Extract the bits of watermark from the middle frequency coefficients of each block;
4. Attach the extracted bits of watermark in order to retrieve the complete watermark.

3. **GA-Based Parameter Amelioration.** In designing a digital image watermarking system, we always encounter two objectives, the fidelity and robustness, which conflict with each other. It usually is a challenging task to maintain both of these properties at the same time. In this study, a genetic algorithm scheme is designed to ameliorate transform parameters in order to achieve the best possible fidelity and robustness, simultaneously.

Figure 2 illustrates the flowchart of the GA which is used to obtain the transform parameters. The initial population of the GA consists of several chromosomes. Each chromosome consists of two real values for the two parameters (β_4, β_8) for each block. In other words, we simulate the transform parameters as chromosomes in the GA evolution process. Furthermore, with the values of the transform parameters in chromosomes, the transform matrix of the PSHT is computed and the embedding procedure is performed.

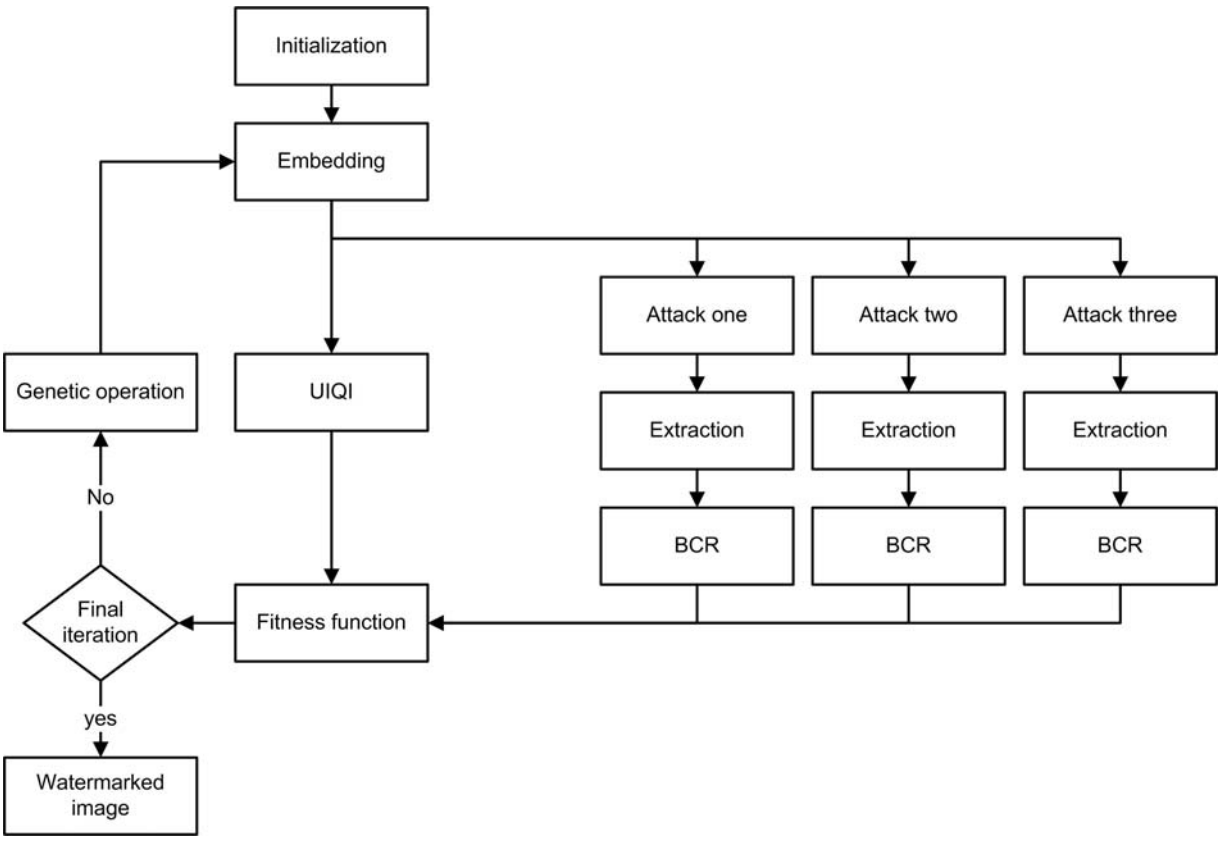

FIGURE 2. Flowchart of transform parameters amelioration using GA

The fidelity and robustness are considered for evaluating the fitness of the chromosomes. There are some criteria for measuring the fidelity such as mean square error and peak signal to noise ratio. However, one of the most effective criteria for robustness evaluation, which also used in this study, is Universal Image Quality Index (IUQI) which is proposed by Wang et al. [31].

On the other hand, for the evaluation of the robustness of our watermarking scheme, and as a result to pick the best the chromosomes, it is necessary to examine how well the watermark could be extracted from the watermarked image even when certain attacks are engaged. In this research, we considered three important types of attacks, namely JPEG compression, median filtering and average filtering.

The parameter for measuring how well the watermark (it is an image itself), is correct after the extraction is called the Bit Correct Ratio (BCR). In this research, the BCR values of the extracted watermark under different attacks are calculated and then, the average of these BCR values is computed and reported as an indication for the robustness of the watermarking scheme [32].

Next, both UIQI and BCR are used to evaluate the fitness of a chromosome in the GA to ameliorate the fidelity and robustness simultaneously. The GA fitness function which

employs both UIQI and BCR parameters and used here is defined as:

$$Fitness\_Function = UIQI + \frac{1}{3}\sum_{i=1}^{3} BCR_i \tag{9}$$

As explained earlier, in the above equation, the $UIQI$ plays the role of fidelity measure, while the BCR plays the role of robustness measure. It is to be noted that the choice of this fitness function has been done to measure the fidelity and robustness but the user may adopt any other quality metrics for his or her applications.

Computing the fitness value, the best chromosomes are picked as the most suitable parents. Then, the next population are generated with crossover and mutation operators. The GA proceeds with this process in each iteration of the algorithm until meeting the terminating condition. Finally, the watermarked image and associated parameters are delivered to the reception side. The mentioned scheme for ameliorating the parameters is summarized in Table 3.

TABLE 3. Summary of transform parameters amelioration

1. Define the fitness function, number of variables, population size, crossover rate, mutation rate and the number of generation;
2. Generate the initial population randomly (transform parameters);
3. Perform the embedding procedure as mentioned in Section 2.3;
4. Compute the UIQI between the original and the watermarked image;
5. Apply the attacks on watermarked image;
6. Extract the watermark from each altered watermarked image;
7. Compute the BCR between the original watermark and extracted one;
8. Evaluate the fitness function for each corresponding solution using Equation (9);
9. Pick chromosomes that have highest fitness values as the parents for the next generation and discard the rest;
10. Apply the genetic operations on the parents and generate the new chromosomes for the next generation;
11. Repeat the Steps 3-11 until the terminal condition is reached;
12. Select the chromosome with the highest fitness value in the final iteration as the ameliorated solution (ameliorated transform parameters).

4. **Experimental Results.** The numerical simulation of our algorithm is implemented using an Intel Pentium IV processor of 3 GHz and 2 GB RAM using Microsoft Windows XP and MATLAB 7.3. We used the original 256×256 gray scale image of Figure 3 and the 64×64 binary watermark image (University of Isfahan emblem) of Figure 4.

The choice of attacks, which is used for evaluating the robustness of watermarking scheme, depends on the application of watermarking scheme. As mentioned before, the employed attacks in our fitness evaluation process are the JPEG compression (quality factor = 50%), median filter (3×3) and average filter (3×3). The JPEG compression is applied as the attacking function because of the popularity of transmitting JPEG images through the Internet. In addition, the median filter is used because this is a popular non-linear spatial filter which is normally used to remove noise spike from an image. The average filter smoothes out image data to eliminate noises. This filter performs spatial filtering on each individual pixel in image using the gray level values in a square window of size 3×3 surrounding each pixel [33].

The number of blocks in our experiments is $\frac{256\times256}{8\times8} = 1024$. Therefore, we have to consider $1024 \times 2 = 2048$ parameters in each chromosome. Choice of the GA parameters is fully arbitrary although it affects the computational cost. Our GA parameters have been tuned according to standard setting as reported in Table 4 [34].

Depending on the orthogonality of the PSHT, which is based on Equation (6) (the elements of transform matrix must be real value), the initial range of transform parameters are set to $[-4, 4]$ and $[-16, 16]$ for β_4 and β_8, respectively. Also, the watermark strength is set to 0.1.

FIGURE 3. The original image

FIGURE 4. The watermark image

TABLE 4. The GA parameters setting

Population size	20480 (10×number of variable)
Creation function	Uniform
Fitness scaling	Proportional
Parents selection	Roulette wheel
Crossover function	Single point
Crossover probability	0.6
Mutation function	Uniform
Mutation rate	0.1
Stopping criteria	500 iteration

In order to show the efficiency of the PSHT domain, we compared the PSHT domain with the method based on the DCT domain. The watermarked images resulted from both the PSHT and DCT schemes are depicted in Figure 5. Based on these images, one can see that the fidelity of the PSHT domain with the parameters evolved by the GA is similar to that of the DCT domain. The UIQI values for the PSHT and DCT domain are 0.9982 and 0.9917, respectively. Therefore, To fairly analyze the results we may assume that the UIQI values between the watermarked image and original one in both algorithms are equal. It is to be noted that the more UIQI, the more similarity between the original and watermarked image.

We use stirmark to estimate the robustness of the schemes [35]. Their corresponding extracted watermarks after mentioned attacks are represented in Figures 6 and 7. These

figures indicate four extracted watermark. The first one is the extracted watermark from the watermarked image which is not altered. The three next ones are the extracted watermark from the watermarked image which is damaged separately by the JPEG compression, median and average filter, respectively. From the BCR values which are depicted under the figures, we can realize that the PSHT domain obtains the extracted watermark with the higher BCR values than the DCT domain (the higher result of the DCT domain on the JPEG compression attack is due to compatibility of the DCT with JPEG compression). To observe the improvement in both the fidelity of watermarked image and the robustness against attacks with the aid of GA, we demonstrate the improvement of the UIQI, BCR and fitness values along with the increase of iteration numbers in Table 5. It is realized that the UIQI, BCR and fitness values increase as the iteration numbers are increased.

(a) $UIQI = 0.9982$ (b) $UIQI = 0.9917$

FIGURE 5. Watermarked images in (a) the PSHT domain and (b) the DCT domain

(a) (b) (c) (d)

FIGURE 6. Extracted watermarks from watermarked image in the PSHT domain: (a) without any attack (BCR = 1.0000), (b) after JPEG attack (BCR = 0.9999), (c) after median attack (BCR = 0.9779) and (d) after average filter attack (BCR = 0.9665) to the watermarked image

TABLE 5. The UIQI and BCR values under different GA iterations

Iteration	UIQI	BCR1	BCR2	BCR3	Fitness value
1	0.8509	0.9075	0.9597	0.9391	1.7863
100	0.8965	0.9188	0.9653	0.9588	1.8441
200	0.9982	0.9999	0.9779	0.9665	1.9796

The major advantages of using the genetic algorithm in digital image watermarking is its high fidelity and good robustness simultaneously; however, the genetic algorithm

(a) (b) (c) (d)

FIGURE 7. Extracted watermarks from watermarked image in the DCT domain: (a) without any attack (BCR = 1.0000), (b) after JPEG attack (BCR = 1.0000), (c) after median attack (BCR = 0.9782) and (d) after average filter attack (BCR = 0.9635) to the watermarked image

spends a lot of time to find the optimum solution. The time needed to perform our program is approximately 250 second per iteration. Thus, the proposed algorithm is not suitable for real time applications.

To demonstrate the robustness of the PSHT scheme, different attacks by applying some typical image processing techniques such as noise addition, cropping, histogram equalization, high pass filtering and scaling are also performed.

4.1. **Noise addition.** The watermarked image is corrupted by the Gaussian noise with zero mean and variance of 500. Then, the watermark is extracted from the attacked watermarked image. The watermarked image after additive noise, and extracted watermark are shown in Figure 8. This figure shows that the quality of extracted watermark is good and therefore, our watermarking method has high robustness against the additive noise attack.

(a) (b)

FIGURE 8. (a) Additive noise attacked image and (b) extracted watermark from attacked image

4.2. **Cropping.** Figure 9 shows a cropped version of the watermarked image in which some part of the image is removed. From the extracted watermark which is presented in this figure, it is concluded that the performance of our scheme against cropping attack is satisfactory.

4.3. **Histogram equalization.** In the evaluation of the histogram equalization attack, the histogram of watermarked image is equalized and then the watermark is extracted. Figure 10 shows the histogram equalized watermarked image and the extracted watermark. It suggests that the proposed scheme is also robust to histogram equalization attack.

(a) (b)

FIGURE 9. (a) Cropped attacked watermarked image and (b) extracted watermark from attacked watermarked image

(a) (b)

FIGURE 10. (a) Histogram equalized attacked watermarked image and (b) extracted watermark from attacked watermarked image

4.4. **High pass filtering.** The robustness of our scheme by sharpening the watermarked image is tested as well. Figure 11 shows the resulting image using a second-order Butterworth high pass filter and the extracted watermark. The result indicates that the proposed method can also survive the high pass filtering attack.

(a) (b)

FIGURE 11. (a) High pass filtered attacked watermarked image and (b) extracted watermark from attacked watermarked image

4.5. **Scaling.** The watermarked image is reduced to half of its original size. In order to extract the watermark, the reduced image is recovered back to its original dimension. The watermarked attacked image and the extracted watermark are shown in Figure 12. The result suggests the high robustness of the proposed watermarking scheme against the scaling attack.

(a) (b)

FIGURE 12. (a) Scaling attacked watermarked image and (b) extracted watermark from attacked watermarked image

These results reveal that the PSHT domain scheme can generate watermarked image with high robustness. In addition, the PSHT domain has some other advantages that make it superior to other domains. The PSHT domain has some parameters that can be used as keys for authorization process. These parameters can also be used in fingerprinting applications. Furthermore, in video watermarking for increasing the security of the watermarking, we can use the PSHT domain with different transform parameters for each frame. In addition, the extraction process needs the transform parameters which is used in the embedding procedure, to extract the watermark properly. Therefore, this dependency on the transform parameters makes the PSHT scheme more secure than other domains.

Although only the Lena image has been used as the original image in the tests, the newly presented watermarking scheme has been implemented in a wide range of original images. All aforementioned results suggest that the GA-based proposed method has potentially high performance for watermarking.

We can also expand the PSHT domain to color images. First, the RGB model of original color image is converted into HIS model. Then the watermark is embedded into I component. Finally, the embedded image can be obtained by converting the watermarked HIS model into RGB model.

5. **Conclusions.** In this paper, digital image watermarking based on parameters amelioration of parametric slant-Hadamard transform using genetic algorithm is presented. The motivation of the present work arises from the necessity of finding out the factors that are responsible for ameliorating the fidelity and robustness of the watermarking. Traditional transforms such as DCT and DWT have the fixed transform matrix which causes the fixed fidelity and robustness. However, the parametric slant-Hadamard transform includes some parameters that are suitable to ameliorate the fidelity and robustness. In different applications, the user can vary the transform parameters empirically to achieve the suitable watermarked image. However, the fidelity and robustness properties, which are conflict with each other, are needed in the most practical applications simultaneously.

Therefore, we apply the genetic algorithm to select the appropriate transform parameters to make a trade off between the fidelity and robustness. In the evolution process, the transform parameters are simulated as chromosomes. A fitness function based on the fidelity and robustness is defined. Then, the GA proceeds to find the suitable transform parameters that maximize the fitness function value. The experimental results show that the GA improves simultaneously the robustness and fidelity of the PSHT domain watermarking scheme and it brings us the scheme closer to an ideal watermarking scheme.

Acknowledgment. The office of graduate studies at the University of Isfahan should be thanked for their support. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] C.-C. Chen and D.-S. Kao, DCT-based zero replacement reversible image watermarking approach, *International Journal of Innovative Computing, Information and Control*, vol.4, no.11, pp.3027-3036, 2008.

[2] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, Digital image steganography: Survey and analysis of current methods, *Signal Processing*, vol.90, no.3, pp.727-752, 2010.

[3] K. Liu and C. Chou, Robust and transparent watermarking scheme for colour images, *IET Image Processing*, vol.3, no.4, pp.228-242, 2009.

[4] C.-C. Chang, C.-C. Lin and Y.-S. Hu, An SVD oriented watermark embedding scheme with high qualities for the restored images, *International Journal of Innovative Computing, Information and Control*, vol.3, no.2, pp.609-620, 2007.

[5] D. Zheng, Y. Liu, J. Zhao and A. E. Saddik, A survey of RST invariant image watermarking algorithms, *ACM Computing Surveys*, vol.39, no.2, 2007.

[6] C. Fei, D. Kundur and R. Kwong, Analysis and design of watermarking algorithms for improved resistance to compression, *IEEE Trans. on Image Processing*, vol.13, no.2, pp.126-144, 2004.

[7] D. Zheng and J. Zhao, Apply phase information in RST image watermarking, *IEEE Int. Conf. on Consumer Electronics*, pp.218-219, 2003.

[8] C. Pun, A novel DFT-based digital watermarking system for images, *Int. Conf. on Signal Processing*, vol.2, 2006.

[9] S. Lin and C. Chen, A robust DCT-based watermarking for copyright protection, *IEEE Trans. on Consumer Electronics*, vol.46, no.3, pp.415-421, 2000.

[10] A. A. Reddy and B. Chatterji, A new wavelet based logo-watermarking scheme, *Pattern Recognition Letters*, vol.26, no.7, pp.1019-1027, 2005.

[11] S. Maity and M. Kundu, DHT domain digital watermarking with low loss in image informations, *AEU – International Journal of Electronics and Communications*, vol.64, no.3, pp.243-257, 2010.

[12] H. Li, S. Wang, W. Song and Q. Wen, Multiple watermarking using Hadamard transform, *Advances in Web-Age Information Management*, pp.767-772, 2005.

[13] X. Zhao, A. Ho, H. Treharne, V. Pankajakshan, C. Culnane and W. Jiang, A novel semi-fragile image watermarking, authentication and self-restoration technique using the slant transform, *Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, vol.1, 2007.

[14] S. Agaian, K. Tourshan and J. Noonan, Parametric slant-Hadamard transforms with applications, *IEEE Signal Processing Letters*, vol.9, no.11, pp.375-377, 2002.

[15] J. Fridrich, Key-dependent random image transforms and their applications in image watermarking, *Int. Conf. on Imaging Science, Systems, and Technology*, vol.99, pp.237-243, 1999.

[16] S. Agaian, K. Tourshan et al., Generalized parametric slant-Hadamard transform, *Signal Processing*, vol.84, no.8, pp.1299-1306, 2004.

[17] A. Latif, A. R. Naghsh-Nilchi and S. A. Monadjemi, A parametric slant-Hadamard system for robust image watermarking, *Journal of Circuits, Systems, and Computers*, vol.19, no.2, pp.451-477, 2010.

[18] M. J. Nassiri, A. Vafaei and A. Monadjemi, Texture feature extraction using slant-Hadamard transform, *International Journal of Applied Science, Engineering and Technology*, vol.3, 2007.

[19] J. Xie, S. Agaian and J. Noonan, Digital watermarking in parametric slant transform domain, *Proc. of SPIE*, vol.6821, 2008.

[20] C. Huang and J. Wu, Watermark optimization technique based on genetic algorithms, *Proc. of SPIE*, vol.3971, pp.516-523, 2000.

[21] F. Shih and Y. Wu, Enhancement of image watermark retrieval based on genetic algorithms, *Journal of Visual Communication and Image Representation*, vol.16, no.2, pp.115-133, 2005.
[22] V. Aslantas, A singular-value decomposition-based image watermarking using genetic algorithm, *AEU – International Journal of Electronics and Communications*, vol.62, no.5, pp.386-394, 2008.
[23] P. Kumsawat, K. Attakitmongcol and A. Srikaew, An optimal robust digital image watermarking based on genetic algorithms in multiwavelet domain, *Trans. on Signal Processing*, vol.5, no.1, pp.42-51, 2009.
[24] J. Xie, S. Agaian and J. Noonan, Secure information hiding algorithm using parametric slant-Hadamard transforms, *Proc. of SPIE*, vol.6982, 2008.
[25] A. Jain, *Fundamentals of Digital Image Processing*, Prentice-Hall, 1989.
[26] S. Agaian, K. Tourshan and J. Noonan, Partially signal dependent slant transforms for multispectral classification, *Integrated Computer-Aided Engineering*, vol.10, no.1, pp.23-35, 2003.
[27] J. Holland, *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*, The MIT Press, 1992.
[28] H. C. Huang, C. M. Chu and J. S. Pan, The optimized copyright protection system with genetic watermarking, *Soft Computing – A Fusion of Foundations, Methodologies and Applications*, vol.13, no.4, pp.333-343, 2009.
[29] C.-C. Chen and C.-S. Lin, A GA-based nearly optimal image authentication approach, *International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.631-640, 2007.
[30] A. Ho, X. Zhu and J. Shen, Slant transform watermarking for digital images, *Proc. of SPIE*, vol.5150, pp.1912-1920, 2003.
[31] Z. Wang and A. Bovik, A universal image quality index, *IEEE Signal Processing Letters*, vol.9, no.3, pp.81-84, 2002.
[32] S. C. Chu, H. C. Huang, Y. Shi, S. Y. Wu and C. S. Shieh, Genetic watermarking for zerotree-based applications, *Circuits, Systems, and Signal Processing*, vol.27, no.2, pp.171-182, 2008.
[33] F. Petitcolas, Watermarking schemes evaluation, *IEEE Signal Processing Magazine*, vol.17, no.5, pp.58-64, 2000.
[34] D. Goldberg et al., *Genetic Algorithms in Search, Optimization, and Machine Learning*, 1st Edition, Addison-Wesley Professional, 1989.
[35] F. A. P. Petitcolas et al., A public automated web-based evaluation service for watermarking schemes: StirMark benchmark, *Proc. of the SPIE/IS&T Conf. on Security and Watermarking of Multimedia Contents*, vol.4314, 2001.