

An Adaptive Digital Image Watermarking Scheme using Fuzzy Logic and Tabu Search

Alimohammad Latif

Electrical and Computer Engineering Department
Yazd University
Yazd, Iran
alatif@yazd.ac.ir

Received March, 2013; revised May, 2013

ABSTRACT. *In this paper, an adaptive digital image watermarking technique using fuzzy logic and tabu search is presented. In our approach, the image is divided into separate blocks and the parametric slant-Hadamard transform is applied on each block individually. Then, the watermark is inserted in the transform domain and the inverse transform is carried out. The selected transform includes some parameters that can be handled to control the requirements of watermarking such as robustness and imperceptibility. The robustness and imperceptibility are in conflict with each other; however, we apply the transform parameters to enhance the robustness by tabu search and after embedding, the watermark is adapted to the image by exploiting the masking characteristics of the human visual system using fuzzy gradient to ensure the imperceptibility. Experimental results show that the proposed technique has high imperceptibility as well as high robustness against variety of attacks.*

Watermarking; Fuzzy Inference System; Fuzzy Gradient; Robustness; Imperceptibility.

1. **Introduction.** The increasingly easy accesses to digital images through the Internet and the increasingly powerful tools available for editing digital images make the authentication of digital images to be a very important issue. One way to resolve it, is to use digital image watermarking. Digital image watermarking is defined as a technique of embedding additional information called watermark into host image by preserving perceptual quality of the host image. The watermark can be detected or extracted for purpose of owner or author identification and integrity verification of watermarked images[1].

A digital watermark can be visible or invisible. A visible watermark typically consists of a visible message or a company logo indicating the ownership of the image. On the other hand, an invisibly watermarked image appears very similar to the host image. The existence of an invisible watermark can be determined using an appropriate watermark extraction or detection algorithm[2].

In most digital image watermarking applications, the watermarked image is likely to be processed in some way before it reaches the receiver. The processing could be lossy compression, additive noise, enhancement and image filtering. An embedded watermark may intentionally or unintentionally be damaged by such a processing. The processed watermarked image is then called attacked watermarked image. The earliest method of attacks uses a trial and error procedure to estimate a combination of pixel values that

has the largest influence on the detector for the least disturbance of the image, and then uses this estimate in order to eliminate the watermark[3].

Digital image watermarking algorithms have some requirements such as imperceptibility and robustness. The imperceptibility presents that the distortion between the host and watermarked image should remain imperceptible. The robustness means the ability of the detector to extract properly the watermark from attacked watermarked image[4].

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 pixel values directly. One of the earliest spatial methods divides an image into two groups and adds a constant value to one group of the image[5]. Another method modifies the pixel information located in the specific position within an image[6]. Spatial based methods have a disadvantage which are fragile to the attacks such as JPEG compression, additive noise and image transforms.

Spectral domain approaches transform the host image into the frequency domain and modulates frequency coefficients to embed the watermark. In general, spectral domain methods are more robust than spatial domain against many common attacks. A fundamental advantage of transform-based techniques is that the image transforms have good energy compactness properties and the most energy of an image can be captured within a relatively small region in the transform domain. The transform basic functions corresponding to these coefficients carry the most perceptually important information of the image. Also, frequency domain watermarking techniques facilitate the process of selecting the most suitable portions of the host image to insert a robust and invisible watermark[7].

Researchers have used some transforms for watermarking applications. Some important transforms are mentioned in the following. Discrete Fourier Transform (DFT) followed by the so-called Fourier-Mellin Transform (FMT), which are the earliest transform that were used in watermarking, can be proven to be rotation, scale and translation invariant[8]. In Premaratne's scheme the watermark is a spread spectrum signal that is embedded in the DFT domain. For watermark detection, the original image is subtracted from the watermarked image and the residual is transformed to the DFT domain where it is highly correlated with the watermark signal[9].

Discrete Cosine Transform (DCT) domain has been used extensively for embedding a watermark. In Suhail's scheme using the DCT, an image is divided into frequency bands, and the watermark can be embedded in low to middle frequency bands. Sensitivities of the Human Visual System (HVS) to changes in those bands have been extensively studied in the context of JPEG compression, and the results of studies can be used to minimize the visual impact of the watermark embedding distortions[10].

Multi-resolution watermarking technique was proposed using Discrete Wavelet Transform (DWT)[11]. Wang et al. decomposed the host image and watermark into sub-bands and then the watermark sequence was embedded into the corresponding level of the transformed image. The proposed sub-band decomposition technique can facilitate placement of the signal in a way that exploits HVS characteristics to obtain imperceptibility[12].

Discrete Hadamard transform (DHT) and its variants were used extensively to develop watermarking algorithms for multimedia signals. Li et al. proposed block-based DHT method where watermark information was inserted into Hadamard coefficients using quantization. The sub-blocks for watermark embedding were selected pseudo randomly to increase security[13]. The DHT domain watermarking methods utilize the benefits such as low computation cost, robust watermark due to the sequencing effect which packs energy of the cover in the low and middle frequency coefficients, and wide length of useful

middle frequency bands with low processing noise which provides compression resilient watermarking at low quality[14].

Slant Transform (ST) was presented for a semi-fragile digital watermarking method for image authentication and self-restoration. Zhao et al. embedded the watermark bits into the middle frequency region of each block after applying slant transform of the original image. The original image is further compressed and then embedded into the least significant bits of the watermarked image for sub-sequent self-restoration. They showed that the slant transform is more robust, accurate and faster than other transform methods based on the DCT and pinned sine transform[15].

The slant transform has the best compaction performance among the non-sinusoidal transforms but it is not optimum in its performance measure among the sinusoidal transforms. In general, there is a trade off between the performance and computational complexity. The need arises for slant transform improvement schemes without incurring their computational complexity. Therefore, Parametric Slant-Hadamard Transform (PSHT) was proposed by Agaian et al. to improve the performance of the slant transform[16].

The our motivation for using the PSHT in watermarking scheme is transform parameters. The transform parameters not only could be applied to change the robustness and imperceptibility but also may be used as private keys to enhance the security of the scheme. Changes on the transform parameters affect both the embedding and extracting procedures. In the former, changes on the transform parameters make some alterations on the robustness and imperceptibility of the scheme. In the latter, changes on the transform parameters causes the untruthful watermark extraction. Authors investigated the need of the proper parameters in extracting procedure by the receiver operating characteristic curve[18]. Also, the simplicity of the PSHT offers a significant advantage in shorter processing time and ease of hardware implementation than most orthogonal transform techniques such as DCT and DWT.

The energy of an image in the spatial domain is uniformly distributed among samples; however, the energy in the transform domain is concentrated in a few samples. We apply Energy Concentration (EC) for comparison of transforms[19]. The energy concentration, which is the ratio of energy of an image in transform domain to special domain, is defined as below:

$$EC(p) = \frac{\sum_{k=1}^p F_k^2}{\sum_{k=1}^{M \times N} f_k^2} \quad (1)$$

where f_k and F_k are the values of the pixels in the spatial and transform domain of the image with the size of $M \times N$, and p is the number of important coefficients. Fig. 1 and 2 illustrate the energy concentration of some transforms on Baboon and Lena (see Fig. 9). The vertical axis is EC and the horizontal axis is the number of important coefficients that used to compute the energy of transformed image. The more coefficients is used, the more energy concentration is obtained. We utilize one to 150 important efficient of transform such as slant, Hadamard, haar and Walsh transform in these figures to compare some transforms to DCT. In PSHT domain (Fig. 1.c and 2.c), some different parameters are used for multiple-betas. It can be seen that the best transform is DCT and the energy concentration of the PSHT is also acceptable.

Xie et al. used the PSHT in digital image watermarking. They partitioned the host image to non-overlap blocks and used a class of adaptive parametric slant bases for each block. They applied spectral spectrum technique in embedding procedure and utilized the average correlation between the extracted watermark and original watermark based on blind extraction algorithm in detection procedure[20].

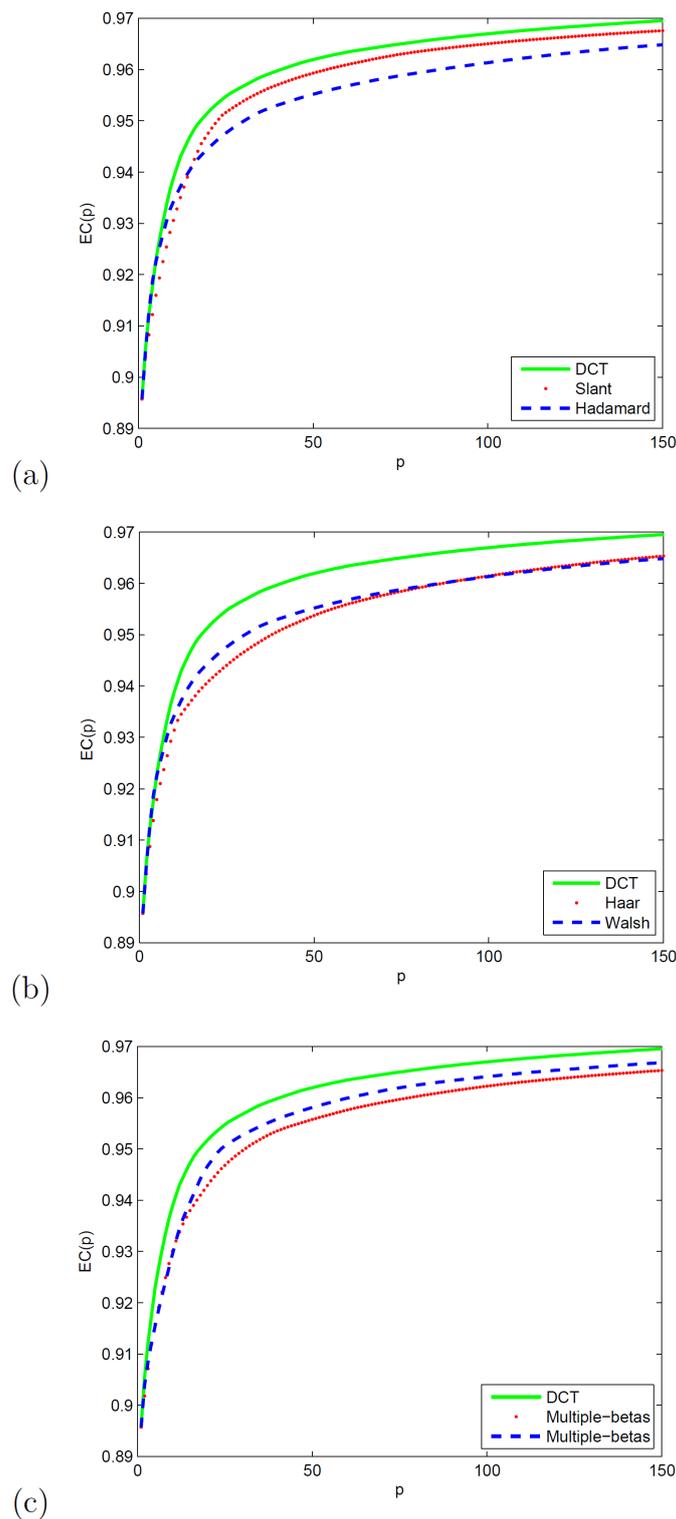


FIGURE 1. Energy conservation on Baboon image

Selection of transform parameters is an important task and Xie applied a sub-optimal solution by working on approximated polynomial of squared error curve against JPEG compression and showed that its robustness performance is comparable with watermarking approaches in other orthogonal domains in the presence of lossy compression. Their

reported results show that the PSHT watermarking scheme has better performance consistently across all compression levels, for both signals that are rich in low frequency components and high frequency components.

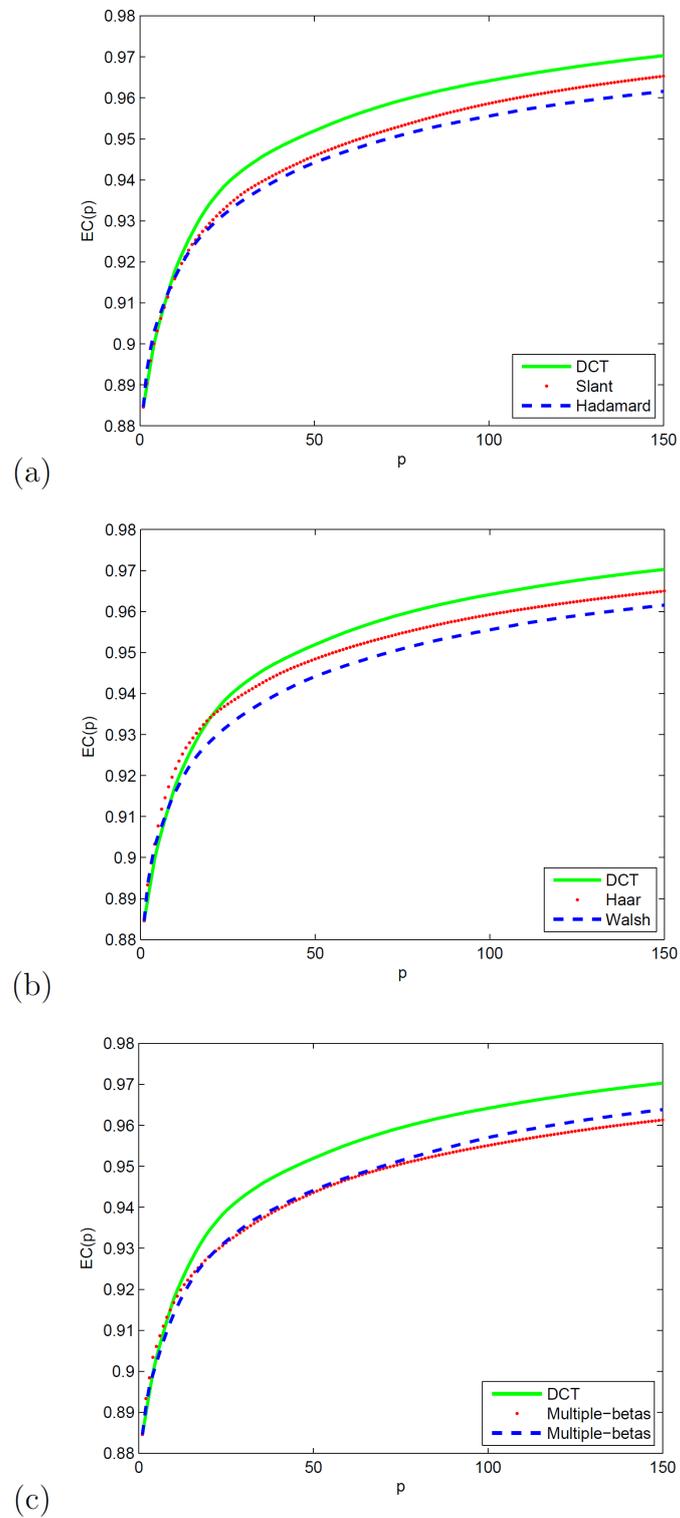


FIGURE 2. Energy conservation on Lena image

The non-linearity of transform parameters and large complexity due to built-in recursion make the solving optimization problem with closed form solution be a difficult task. Authors resolved the problem via the genetic algorithm by definition of a proper fitness function[18]. The genetic algorithm searches for the optimal transform parameters to improve the performance of watermarking algorithm[21]. One of the main advantages of using the genetic algorithm is its high imperceptibility and good robustness simultaneously; however, the genetic algorithm spends a lot of time to find the optimum solution.

In this study, in order to enhance the robustness against some attacks as well as imperceptibility, selection of the parameters is performed by Tabu Search (TS), to improve the robustness against malicious attacks[22]. Finally, the imperceptibility is enhanced by applying the masking characteristics of the HVS using fuzzy gradient. After implementing the proposed method, we evaluate and compare the performance of our scheme with discrete cosine transform domain.

The rest of this article is organized as follows. A brief overview of the PSHT and TS is described in section 2 and 3 respectively. In the next section, we discuss the procedures of proposed watermarking scheme. Section 5 is dedicated to the presenting of the experimental results. Moreover, the performance of our algorithm against some common attacks is evaluated. Finally, the conclusion remarks are given in the last section.

2. Parametric Slant Hadamard Transform. Let f represents the original image and F the transformed image, the 2D PSHT is given by:

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

where S_{2^n} represents a $2^n \times 2^n$ parametric slant-Hadamard matrix with real numbers and T denotes the transpose. The inverse transformation to recover f from the transform components matrix, F , is given by:

$$f = S_{2^n}^T F S_{2^n} \tag{3}$$

The parametric slant-Hadamard matrix of order 2^n is generated in terms of matrix of order 2^{n-1} using Kronecker product operator \otimes [23], as:

$$S_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4}$$

$$S_{2^n} = \frac{1}{\sqrt{2}} Q_{2^n} (I_2 \otimes S_{2^{n-1}}), n > 1 \tag{5}$$

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

$$Q_{2^n} = \begin{pmatrix} 1 & 0 & \vdots & 0_{2^{n-1}-2} & \vdots & 1 & 0 & \vdots & 0_{2^{n-1}-2} \\ a_{2^n} & b_{2^n} & \dots & \dots & \dots & -a_{2^n} & b_{2^n} & \dots & \dots \\ \dots & \dots \\ 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} & \vdots & 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} \\ \dots & \dots \\ 0 & 1 & \vdots & 0_{2^{n-1}-2} & \vdots & 0 & -1 & \vdots & 0_{2^{n-1}-2} \\ -b_{2^n} & a_{2^n} & \dots & \dots & \dots & b_{2^n} & a_{2^n} & \dots & \dots \\ \dots & \dots \\ 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} & \vdots & 0_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} & \vdots & I_{2^{n-1}-2} \end{pmatrix} \tag{6}$$

and the parameters a_{2^n} and b_{2^n} are obtained recursively by:

$$a_{2^n} = \sqrt{\frac{3(2^{2n-2})}{4(2^{2n-2}) - \beta_{2^n}}} \quad b_{2^n} = \sqrt{\frac{2^{2n-2} - \beta_{2^n}}{4(2^{2n-2}) - \beta_{2^n}}} \quad (7)$$

Depending on the

β_{2^n} values, the PSHT falls into one of the four categories below:

1. $\beta_4 = \beta_8 = \dots = \beta_{2^n} = \beta = 1$ results the classical slant transform.
2. $\beta_{2^n} = 2^{2n-2}$ for all β_{2^n} , $n \geq 2$ results the Walsh-Hadamard transform.
3. $\beta_4 = \beta_8 = \dots = \beta_{2^n} = \beta$, $|\beta| \leq 4$ results the constant-betas slant transform.
4. $\beta_4 \neq \beta_8 \dots \neq \beta_{2^n}$, $-2^{2n-2} \leq \beta_{2^n} \leq 2^{2n-2}$, $n = 2, 3, 4 \dots$ results the multiple-betas slant transform.[24, 25]

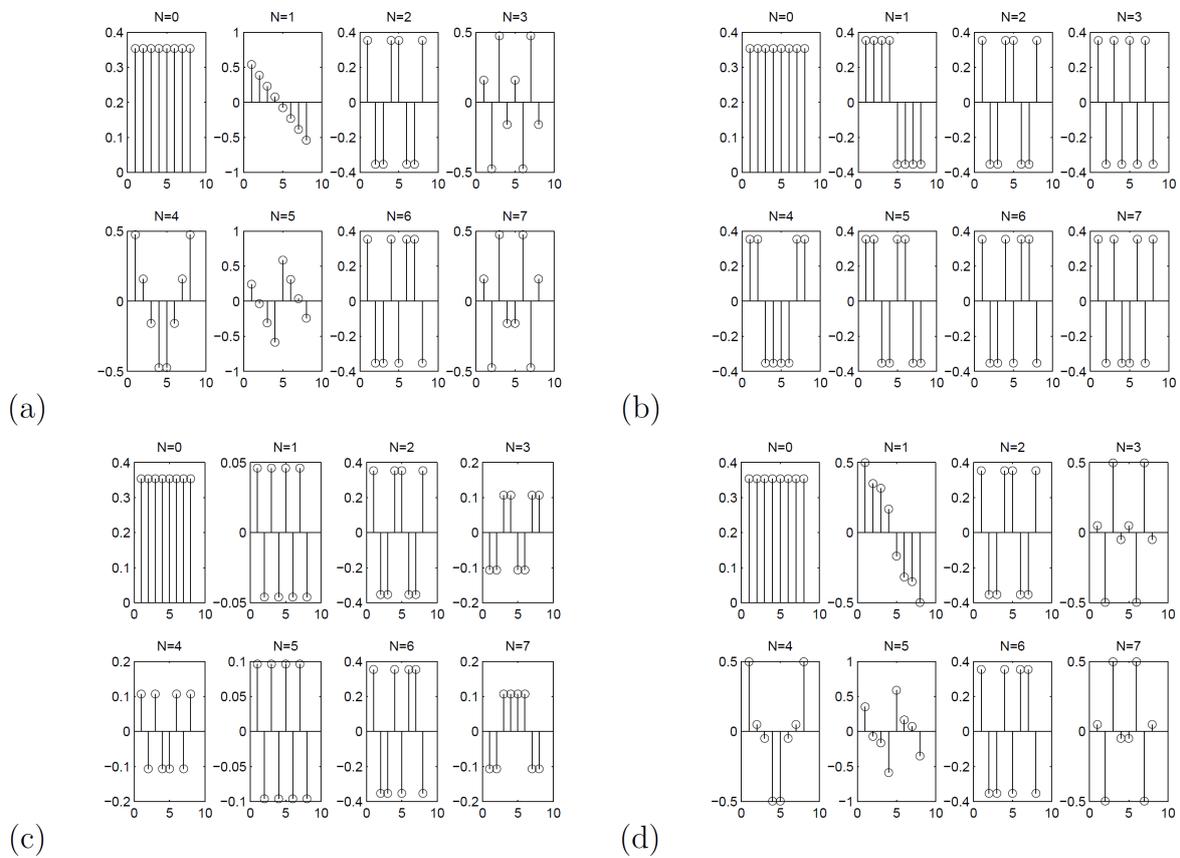


FIGURE 3. Basic patterns (a) Classical slant (b) Walsh-Hadamard (c) Constant-betas slant (d) Multiple-betas slant.

In the multiple-betas slant transform, some values of β_{2^n} can be equal but not all of them. Fig. 3 shows the parametric slant-Hadamard basic patterns for the classical ($\beta_4 = 1, \beta_8 = 1$), Walsh-Hadamard ($\beta_4 = 4, \beta_8 = 16$), constant-betas ($\beta_4 = 2.2, \beta_8 = 2.2$), and multiple-betas ($\beta_4 = -4.1, \beta_8 = 10.2$) slant transform of size 8. The parameters in constant-betas and multiple-betas slant transform are chosen by TS so that the proposed watermarking scheme obtains high robustness.

Selection of transform parameters, which is β_{2^n} ; $n \geq 2$, plays an important role in satisfying the requirements of watermarking[17]. Each parameter varies in predefined

interval for necessary condition of orthogonality. By defining an appropriate fitness function, authors investigated the impact of parameters on imperceptibility and robustness of watermarking algorithm[18].

3. Tabu search. Tabu search is the meta-heuristic approach, which has important links to evolutionary methods. The adaptive memory feature of TS allows to implement the procedures that are capable of searching the solution space economically and effectively. TS uses attributive memory for guiding purposes. This type of memory records information about solution attributes which causes moving from one solution to another. The emphasis on responsive exploration in TS, whether in a deterministic or probabilistic implementation, derives that a bad strategy choice can yield more information than a good random choice[26].

TS can be applied directly to verbal or symbolic statements of many kinds of decision problems, without the need to transform them into mathematical formulation. TS begins in the same way as ordinary local or neighborhood search, proceeding iteratively from one point (solution) to another until a chosen termination criterion is satisfied. Each $x \in X$ has an associated neighborhood $N(x) \subset X$, and each solution $x' \in N(x)$ is reached from x by a move operation.

This class of problem is characterized as optimizing (minimizing or maximizing) a function $h(x)$ subject to $x \in X$, where $h(x)$ may be linear or non-linear. Such a method only permits moves to neighbor solutions that improve the current objective function value and ends when no improving solutions can be found. A pseudo-code of a generic ascent is presented in the following:

1. Choose $x \in X$ to start the process.
2. Find $x' \in N(x)$ such that $h(x') > h(x)$.
3. If no such x' can be found, x is the local optimum and the method stops.
4. Otherwise, designate x' to be the new x and go to 2[27].

4. Method. According to the embedding rule which is used in watermarking procedure, the watermark is often additive or multiplicative. To get better performance in terms of robustness and imperceptibility, both mentioned methods are used in the transform domain. In the present work, we adopt additive approach in the PSHT domain by fuzzy gradient.

Fig. 4 shows the general structure of the proposed embedding algorithm. Our embedding technique includes three main steps: image transformation, watermark embedding and adaptive enhancement of imperceptibility. In the image transformation stage, the host image is divided into 8×8 non-overlapped blocks and the PSHT of each block is computed. Afterwards, in the watermark embedding stage, the middle frequency band of each block is modulated using the following equation[28]:

$$F_W = F + \lambda * W \quad (8)$$

where F and F_W are the transforms of the host and watermarked image respectively, λ is the embedding strength and W is the watermark. Then, the inverse PSHT is carried out and the watermarked image, F_W , is returned to f_w , which is the watermarked image in the spatial domain.

Watermark embedding on the coefficients of the PSHT makes some alterations on the whole image, even in regions where a signal of that particular frequency is not actually present. Thus, in such regions the watermark fails to be masked. Therefore, in the third stage of our procedure, which is adaptive enhancement of imperceptibility, the special

mask is exploited to adapt the watermark to the watermarked image[29]. The host image, f , and the watermarked image, f_W , are added pixel by pixel according to a local weighting factor, $\alpha_{(i,j)}$, resulted a new watermarked image, f'_W as:

$$f'_W(i, j) = f(i, j)(1 - \alpha_{(i,j)}) + \alpha_{(i,j)}f_w(i, j) \quad (9)$$

or

$$f'_W(i, j) = f(i, j) + \alpha_{(i,j)}(f_w(i, j) - f(i, j)) \quad (10)$$

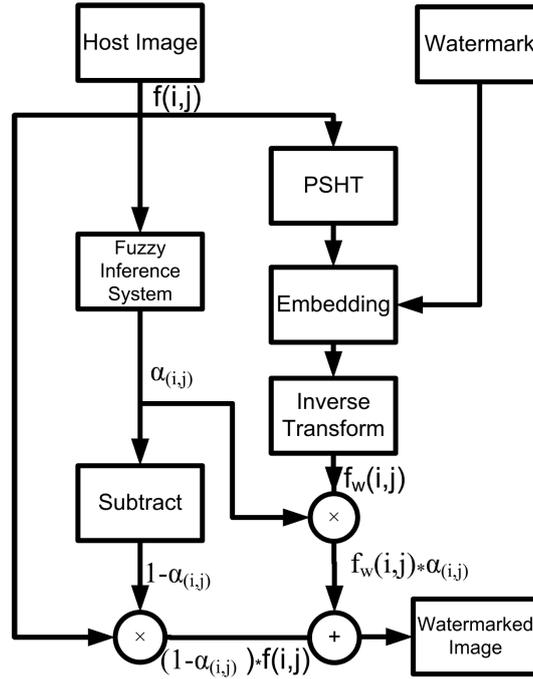


FIGURE 4. Flowchart of the embedding procedure.

The local weighting factor, $\alpha_{(i,j)}$, considers the characteristics of human eyes to enhance the imperceptibility. This is helpful in edges, where the embedding of watermarking data is easier. Here, $\alpha_{(i,j)}$ is considered about one which results $f'_W(i, j) \approx f_w(i, j)$. In regions that are more sensitive to changes, the insertion of the watermark is more disturbing. Thus, $\alpha_{(i,j)}$ is considered about zero which results $f'_W(i, j) \approx f(i, j)$.

It is an important task to choose an appropriate visual characteristic of the image on the basis of which the local weighting factor $\alpha_{(i,j)}$ changes. According to the capability of fuzzy set theory of performing complex non-linear mappings between input and output spaces, we use fuzzy inference system to estimate the local weighting factor for each pixel. In the next section, we apply gradient and fuzzy inference system to compute fuzzy gradient as the local weighting factor.

The watermark extraction process needs the transform coefficients of the host and watermarked images. Thus, one needs proper parameters of transform that computes the transform coefficients. If these parameters are not the same which have been used in the embedding process, the watermark will not be extracted successfully. The watermark extraction procedure is based on the reverse computation of Eq. 8, which is shown below:

$$W = \frac{1}{k}(F_W - F) \tag{11}$$

After the extraction of the pieces of watermark from each block, these pieces are concatenated and the meaningful watermark is obtained.

4.1. Gradients. For each pixel $f(i, j)$ of the image (apart from the border pixels), we use a 3×3 neighborhood window as illustrated in Fig. 5. Each element in 3×3 window corresponds to a particular direction such as North West (NW), North (N), North East (NE), West (W), East (E), South West (SW), South (S) and South East (SE). If f is denoted as the input image, the gradient $\nabla_{(k,l)}f(i, j)$ is defined as:

$$\nabla_{(k,l)}f(i, j) = f(i + k, j + l) - f(i, j) \quad k, l \in \{-1, 0, 1\} \tag{12}$$

where the pair (k, l) corresponds to one of the eight directions and (i, j) is called the center of the gradient, and the eight gradients are called the basic gradients[30, 31].

The gradient which is computed diagonally is relative gradient. The basic gradient, $\nabla_{(-1,-1)}f(i, j)$, plus the two relative gradients, $\nabla_{(-1,-1)}f(i - 1, j + 1)$ and $\nabla_{(-1,-1)}f(i + 1, j - 1)$, in NW direction are shown in Fig. 6.

-1	0	1	
NW	N	NE	-1
W	(i, j)	E	0
SW	S	SE	1

FIGURE 5. The neighborhood of central pixel.

-2	-1	0	1	
				-2
	NW		NE	-1
		(i, j)		0
	SW			1

FIGURE 6. The basic gradient and two relative gradients in NW direction.

An overview of the involved gradients are given in Tab.1. Each direction in column 1 corresponds to a position with respect to a given central position. Column 2 gives the basic gradient for each direction, while column 3 and 4 show the two relative gradients. We denote the basic gradient as $\nabla_R f(i, j)$, while the two related gradient values were entitled as $\nabla'_R f(i, j)$ and $\nabla''_R f(i, j)$, respectively.

TABLE 1. The basic gradient and the first and second relative gradients.

Direction	$\nabla_R f(i, j)$	$\nabla'_R f(i, j)$	$\nabla''_R f(i, j)$
NW	$\nabla_{(-1,-1)} f(i, j)$	$\nabla_{(-1,-1)} f(i+1, j-1)$	$\nabla_{(-1,-1)} f(i-1, j+1)$
N	$\nabla_{(0,-1)} f(i, j)$	$\nabla_{(0,-1)} f(i, j-1)$	$\nabla_{(0,-1)} f(i, j+1)$
NE	$\nabla_{(1,-1)} f(i, j)$	$\nabla_{(1,-1)} f(i-1, j-1)$	$\nabla_{(1,-1)} f(i+1, j+1)$
E	$\nabla_{(1,0)} f(i, j)$	$\nabla_{(1,0)} f(i-1, j)$	$\nabla_{(1,0)} f(i+1, j)$
SE	$\nabla_{(1,1)} f(i, j)$	$\nabla_{(1,1)} f(i-1, j+1)$	$\nabla_{(1,1)} f(i+1, j-1)$
S	$\nabla_{(0,1)} f(i, j)$	$\nabla_{(0,1)} f(i, j-1)$	$\nabla_{(0,1)} f(i, j+1)$
SW	$\nabla_{(-1,1)} f(i, j)$	$\nabla_{(-1,1)} f(i-1, j-1)$	$\nabla_{(-1,1)} f(i+1, j+1)$
W	$\nabla_{(-1,0)} f(i, j)$	$\nabla_{(-1,0)} f(i-1, j)$	$\nabla_{(-1,0)} f(i+1, j)$

4.2. Fuzzy Gradient. In this section, a fuzzy inference system is designed to estimate fuzzy gradient adaptively as the local weighting factor, $\alpha_{(i,j)}$, for watermark embedding procedure. Fuzzy inference system is a mechanism for formulating and transferring human expert knowledge into real word applications[32]. Recently fuzzy inference engine has been widely used in several intelligent multimedia applications. Fuzzy inference system provides a flexible tool for modeling the relationship between input and output information. Linguistic fuzzy sets and conditional statements allow systems to make decisions based on imprecise or incomplete information.

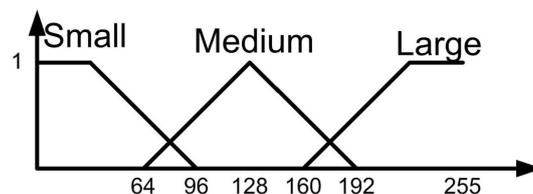


FIGURE 7. The input membership function.

In each fuzzy inference system four main component should be considered: a fuzzifier, a fuzzy inference engine, a fuzzy rule base and a defuzzifier[33]. The fuzzifier maps crisp inputs to fuzzy sets defined on the input space. Fuzzy sets can be represented by a membership functions. A membership function is a curve that defines how each point in the input space is mapped to a membership value between zero and one. There is a wide selection of membership function to choose from. The only condition a membership function must be really satisfied is that it must vary between zero and one. The fuzzy inference engine combines the statements in the rule base to produce a mapping from fuzzy sets in the input space to fuzzy sets in the output space. The core of fuzzy inference system is its knowledge base, which is expressed in the fuzzy rules. Each rule can be described as If - Then rules such as fuzzy Mamdani type:

If x is A THEN y is B

where A and B are linguistic values defined by fuzzy sets on the ranges X and Y , respectively. The If-part of the rule is called the antecedent, while the Then-part is called the consequent.

After the fuzzy rules are applied, the output should be defuzzified. In other words, the defuzzifier stage maps fuzzy consequent into crisp output values. One of the commonly used defuzzification method is the centroid defuzzification method which is computed as:

$$\alpha = \frac{\sum_{i=1}^s \mu(z_i) \cdot z_i}{\sum_{i=1}^s \mu(z_i)} \tag{13}$$

where s is the number of rules, z_i is the output at rule i , and $\mu(z_i)$ is the membership value in the fuzzy set[34].

The simplest membership functions are formed using straight lines. In this study, we use a membership function for absolute value of the basic and two relative gradients of a pixel with linguistic variables: Small, Medium and Large. This input membership function is shown in Fig. 7.

The horizontal axis of this function represent all the possible absolute gradient values which is in the range of [0 - 255]. A membership degree indicates the degree in which a certain gradient value matches the predicate. For example, if a gradient value has membership degree one in the fuzzy set Large, it means that it is Large for sure. The gradient value which is labeled Large, means the grey level of the central pixel of a neighborhood differs from its neighbors.

According to the membership function, (see Fig. 7) we may conclude that the gradient values for a given direction R , which are situated in the interval [0 - 96] and belong to the homogeneous regions are labeled as Small. The gradient values for a given direction R , which are situated in the interval [96 - 192] and are not exactly belong to the non-homogeneous or homogeneous regions are labeled as Medium. Finally the gradient values for a given direction R , which are situated in the interval [192 - 255] and belong to the non-homogeneous regions are labeled as Large.

TABLE 2. The important proposed fuzzy rules.

Rule Number	$ \nabla_R f(i, j) $	$ \nabla'_R f(i, j) $	$ \nabla''_R f(i, j) $	$\nabla^{FG}_R f(i, j)$
1	Large	Large	Large	Large
2	Large	Large	Small	Large
3	Large	Small	Large	Large
4	Large	Small	Small	Medium
5	Small	Large	Large	Medium
6	Small	Large	Small	Medium
7	Small	Small	Large	Medium
8	Medium	Medium	Medium	Medium
9	Medium	Large	Small	Medium
10	Medium	Small	Large	Medium
11	Small	Small	Small	Small
12	Medium	Small	Small	Small

Watermarking schemes which are based on HVS are content-dependent and consequently are inherently more robust to attacks. Therefore, we state the rules based on HVS. The basic HVS knowledge can be described as Mamdani IF - THEN rules in fuzzy inference system[35]. In HVS, there are several characteristics of image that affect human visual observation. The observations and experiments indicate that disturbances are much less visible in highly textured regions than in the uniform areas. Also, contours are more sensitive to additive noise than highly textured regions, but less than flat areas; and disturbances are less visible over dark and bright regions. Based on the above considerations,

the larger the gradient, the less sensitive HVS to the changed degree of the elements of the host image. Therefore, the local weighting factor would be higher and vice versa.

The important proposed rules based on HVS are summarized in Tab.2. Each rule has three antecedent and one consequent. The multiple parts of antecedent use AND operator. We use the classical operator for AND which is minimum function. In this table, column 1 is the basic gradient value, column 2 and 3 are the two relative gradients value and column 4 is fuzzy gradient for direction R. For example, the first rule indicates that:

IF absolute value of the basic gradient is Large AND
 absolute value of the first relative gradient is Large AND
 absolute value of the second gradient is Large
 THEN the fuzzy gradient is Large.

The first three rules are dealing with Large value for the first gradient and one of the relative gradients. The pixels with these characteristics are considered as an edge in the image and the local weighting factor for these pixels would be Large. The next seven rules relate to the pixels that the value of gradients demonstrate that these pixels do not exactly belong to the non-homogeneous or homogeneous region, therefore the local weighting factor for these pixels are set Medium. In homogeneous regions, we will obtain smaller value of gradients, which will cause much sensitive to HVS. The last group of the rules is related to the pixels that belongs to the homogeneous region that means these pixels seem to be similar to their neighborhood and the local weighting factor would be low.

The fuzzy inference engine is an important part of the system. There are a number of different ways to implement the fuzzy inference engine. Max-Min inference method is used in this paper. The fuzzy rules and membership functions were developed using intuitive logic to make the output of fuzzy system. The membership function of Small, Medium and Large for fuzzy gradient (output space) is indicated in Fig. 8. The output of the fuzzy inference system is a single value which corresponds to the fuzzy gradient for each pixel in each direction.

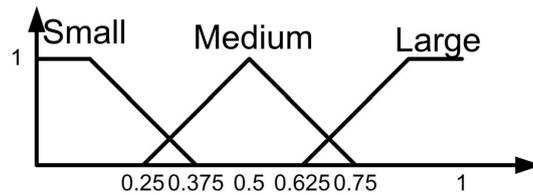


FIGURE 8. The output membership function.

The fuzzy gradients $\nabla_R^F f(i, j)$ for each pixel in eight directions R ($R \in \{NW, N, NE, E, SE, S, SW, W\}$) are calculated and then, the maximum value of eight fuzzy gradients in eight directions is considered as fuzzy gradient for each pixel.

$$\nabla^{FG} f(i, j) = \max_R \nabla_R^{FG} f(i, j) \quad (14)$$

In this equation $\nabla^{FG} f(i, j)$ corresponds to the fuzzy gradient for pixel at the position of (i, j) and $\nabla_R^{FG} f(i, j)$ indicates the fuzzy gradient in direction R for pixel at the position of (i, j) . The final fuzzy gradient that is computed in the above equation is used as local weighting factor, $\alpha_{(i,j)}$, for each pixel individually. The algorithm for computing the local weighting factor for each pixel can be summarized in Tab.3.

TABLE 3. Summarized the algorithm for computing the local weighting factor for each pixel.

1. Consider the pixels from the 3×3 neighborhood around $f(i, j)$;
2. Compute the gradients of eight directions around central pixel;
3. Fuzzify the gradients based on the membership functions;
4. Pass the gradients as fuzzy inputs to the fuzzy inference engine;
5. Compute the fuzzy gradient for eight directions based on fuzzy rules;
6. Select the maximum value of eight fuzzy gradients.

5. Numerical Example. In order to evaluate our proposed watermarking scheme, we use 512×512 host grey scale images of Fig. 9. The images are identified by name: Baboon, Lena. Baboon represents images with large areas of complex texture and homogeneous areas; Lena has a mixture of characteristics such as smooth background, complex textures and big curves. The University of Isfahan logo which is 64×64 binary image is used as the watermark (see Fig. 10). The numerical simulations are implemented using an Intel Core Duo CPU T2450 of 2.00 GHz and 2 GB RAM and MATLAB 2011.

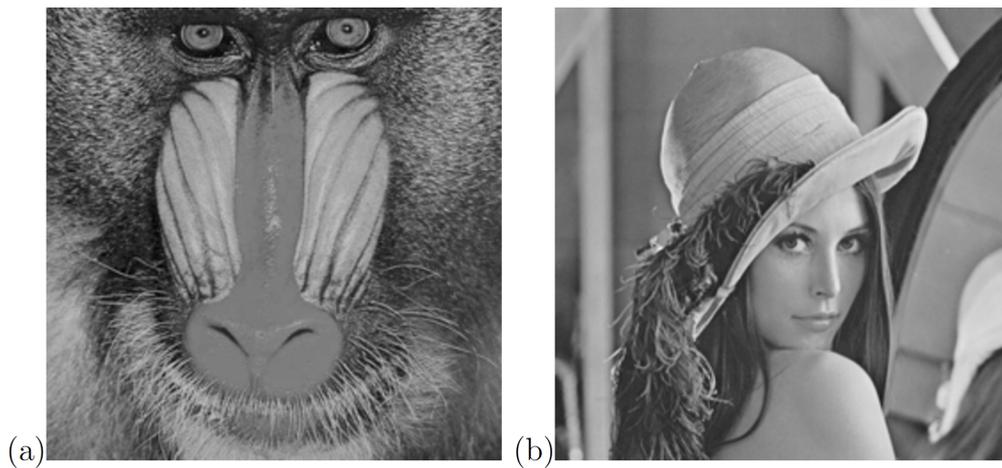


FIGURE 9. Host images (a) Baboon (b) Lena.



FIGURE 10. The watermark image.

we apply tabu search to select the transform parameters that maximize the robustness of approach against JPEG compression (quality factor = 80), additive noise (gaussian noise with zero mean and variance of 100), histogram equalization, high pass filtering (second-order Butterworth filter) and scaling (scale = 2) attacks[36]. In TS the function, which must be maximized, is the summation of Bit Correct Ration (BCR) against the mentioned attacks. The BCR is a numeric criteria that measure the correction rate of the extracted watermark. The BCR is accuracy indicator for retrieved watermark as well

as for robustness evaluation more precisely. The formula of the BCR is demonstrated as follows:

$$BCR = \frac{\sum_{i=1}^L \overline{W_i \oplus W'_i}}{L} \times 100 \quad (15)$$

where W_i is the i th binary value in the bit stream of the original watermark, W'_i is the i th binary value in the bit stream of the extracted watermark, \oplus represents exclusive-OR operation, and L is the length of the watermark. Obviously, when the BCR is higher, the similarity between original and extracted watermark is higher[37].

We use the transform parameters, which are evolved by TS, in the embedding procedure. The simulation of fuzzy inference system for Lena, which is used in the embedding procedure, is shown in Fig. 11. To show the results precisely, we present the values in $[0, 255]$. This figure implies that the edge areas have more fuzzy gradient and the homogeneous areas have less fuzzy gradient. In the next sub-sections, we will first demonstrate the imperceptibility and then the robustness of the proposed method against mentioned attacks.



FIGURE 11. (a) The original image (b) The fuzzy gradient value.

6. Discussion.

6.1. Imperceptibility. The embedding algorithm is repeated four times by the parameters in classical, Walsh-Hadamard, constant-betas, and multiple-betas slant transform categories. The transform parameters in constant-betas and multiple-betas are obtained by tabu search. The watermarked images are demonstrated in Fig. 12-15. These results implicate that the watermark has not imposed any obvious degradation to the host image. In comparison, the embedding algorithm is also implemented in DCT domain. The outcome in DCT domain is also demonstrated in Fig. 16.

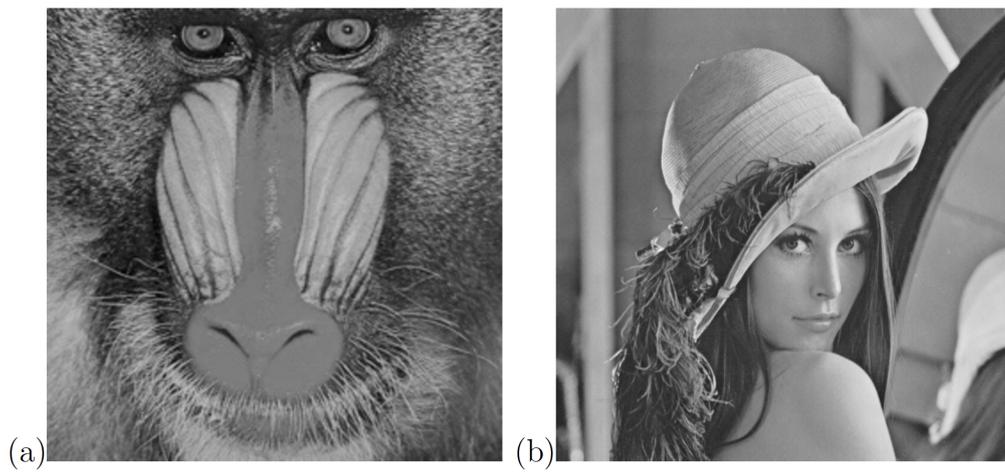


FIGURE 12. Watermarked image in classical slant.

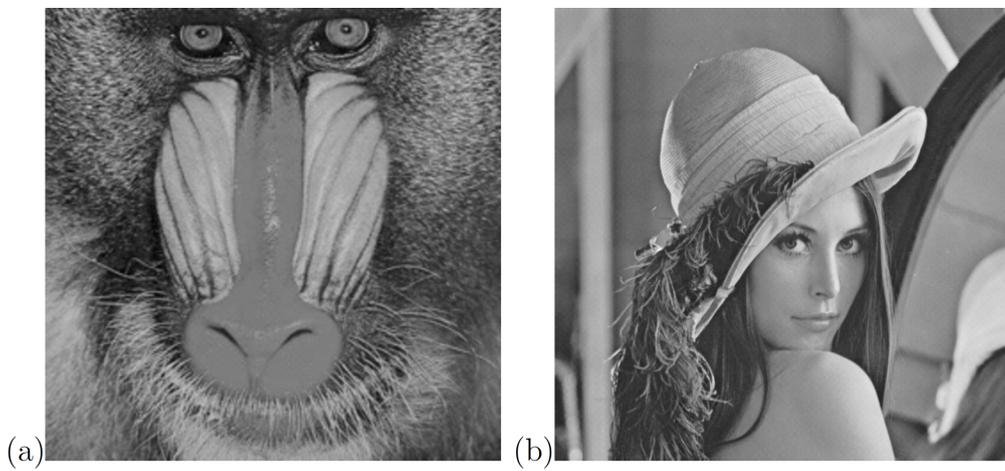


FIGURE 13. Watermarked image in Walsh-Hadamard.

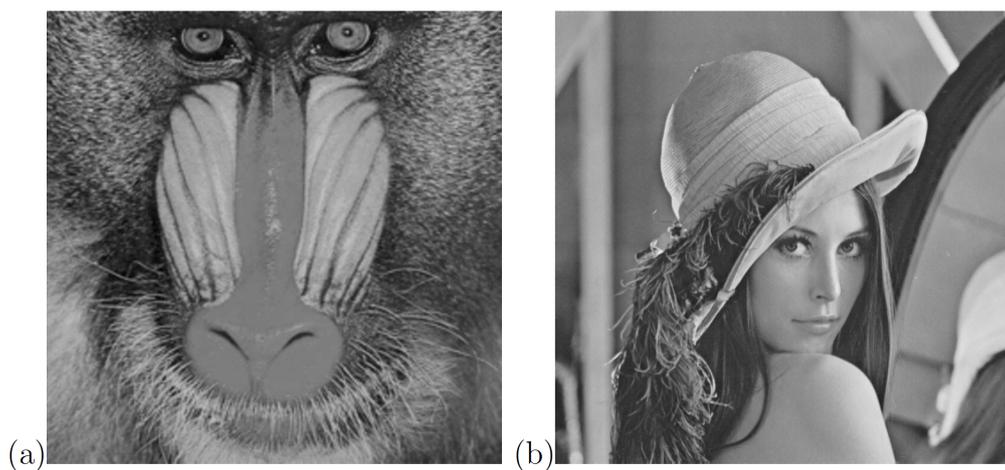


FIGURE 14. Watermarked image in constant-betas slant.

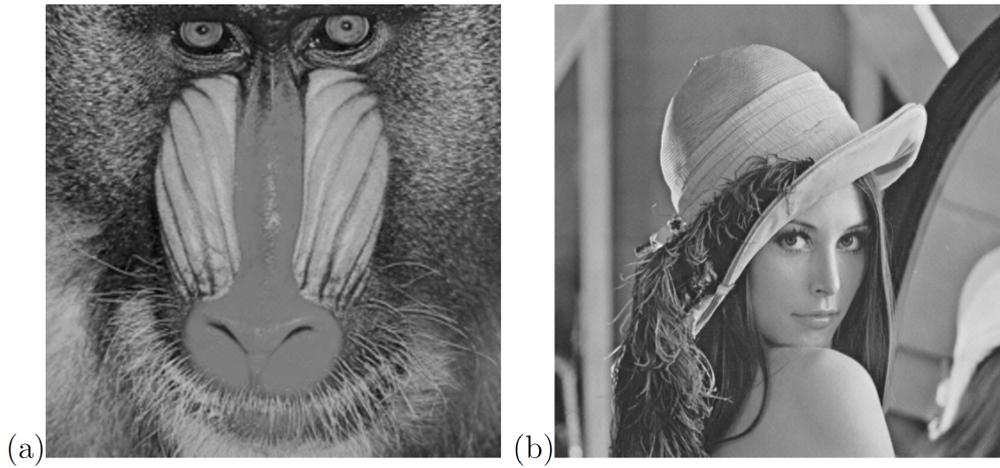


FIGURE 15. Watermarked image in multiple-betas slant.

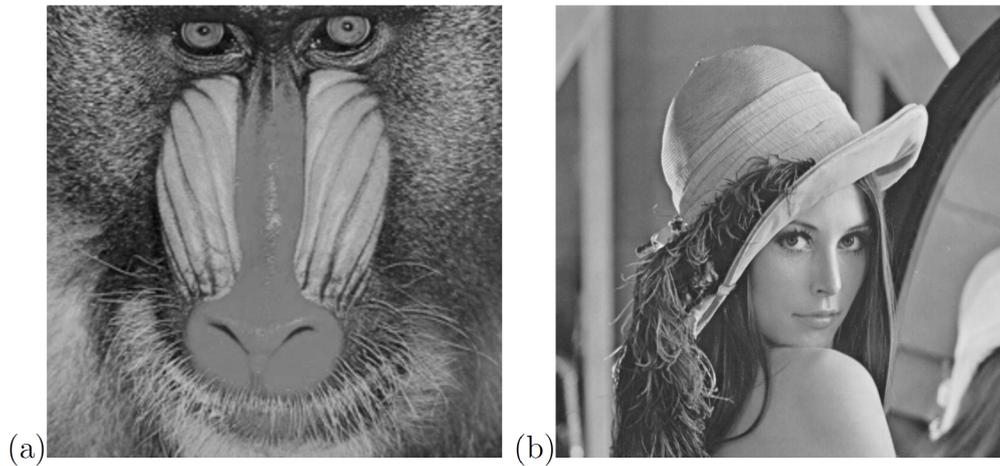


FIGURE 16. Watermarked image in DCT domain.

TABLE 4. The PSNR and BCR for watermarked images.

Image	Classical slant		Walsh-Hadamard		Constant-betas		Multiple-betas		DCT domain	
	PSNR	BCR	PSNR	BCR	PSNR	BCR	PSNR	BCR	PSNR	BCR
Baboon	50.812	100	48.954	100	51.245	100	52.187	100	43.056	100
Lena	51.319	100	49.197	100	52.756	100	53.321	100	43.043	100

We calculate Peak Signal to Noise Ratio (PSNR) as a quality indicator for watermarked images. The PSNR criteria is defined as:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{E} \right)_{db} \quad (16)$$

where E is the mean square error between the original and watermarked image as defined in the following:

$$E = MSE(f', f'_w) = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f(i, j) - f'_w(i, j))^2 \quad (17)$$

where $f(i, j)$ and $f'_w(i, j)$ denote the (i, j) th pixel values in the original image and watermarked image respectively. It is clear that if the PSNR is higher, the similarity between the host and watermarked image is higher[38]. Tab.4 compares the performance of the classical slant, Walsh-Hadamard, constant-betas, multiple-betas slant transform and DCT on the mentioned images. It can be observed that the proposed algorithm possesses high perceptual quality in addition with excellent watermark extraction. The values of BCR indicate that the extracted watermarks are like to the original one. Also, compared with the DCT domain, the proposed scheme achieves extremely much higher PSNR.

6.2. Robustness. In a robust watermarking scheme, attacks cannot affect the embedded watermark, and the BCR between original watermark and attacked extracted watermark would be high. We use stirmark to estimate the robustness of our scheme. We performed different attacks by applying some typical image processing techniques such as JPEG compression, additive noise, histogram equalization, high pass filtering and scaling attacks on watermarked images.

6.2.1. JPEG Compression. The watermarked image is compressed using JPEG algorithm[39]. The reason for applying the JPEG compression as the attacking function is due to the popularity of transmitting JPEG images under the Internet. Fig. 17 shows the extracted watermark of proposed scheme on Lena and Baboon images after JPEG compression. It indicates that the robustness of our scheme against JPEG compression does not decrease the quality of extracted watermark very much.

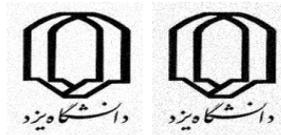


FIGURE 17. Extracted watermarks from Baboon and Lena after JPEG compression attack respectively.

6.2.2. Noise Addition. We evaluate the robustness of our algorithm by additive Gaussian noise on the watermarked images. Fig. 18 shows the extracted watermark from Lena and Baboon watermarked images which were corrupted by the Gaussian noise with zero mean and variance of 100. The extracted watermarks have been shown that the adaptive proposed method has high robustness against additive noise attack.

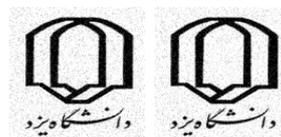


FIGURE 18. Extracted watermarks from Baboon and Lena after additive noise attack respectively.

6.2.3. Histogram Equalization. Histogram of watermarked images are equalized and then, the watermarks are extracted. Fig. 19 shows the extracted watermarks from Lena and Baboon watermarked images after histogram equalization attacks. It suggests that the adaptive proposed scheme is also robust to histogram equalization attack since the similarity between the original watermark and extracted watermarks are acceptable.

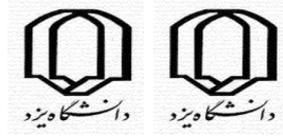


FIGURE 19. Extracted watermarks from Baboon and Lena after histogram equalization attack respectively.

6.2.4. *High Pass Filtering.* We are also going to test the robustness by sharpening the watermarked images. Fig. 20 shows the extracted watermarks from Lena and Baboon watermarked images after a second-order Butterworth high pass filter. The test result indicates that our proposed method can also survive the high pass filtering attack.

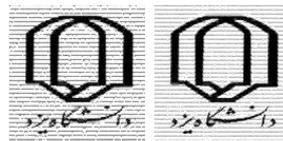


FIGURE 20. Extracted watermarks from Baboon and Lena after high pass filtering attack respectively.

6.2.5. *Scaling.* The watermarked images are reduced to half of their original size. In order to detect the watermark, the reduced images are recovered back to their original dimension. The extracted watermarks from Lena and Baboon watermarked images are shown in Fig. 21. The results again suggest the high performance of our adaptive watermarking scheme.



FIGURE 21. Extracted watermarks from Baboon and Lena after scaling attack respectively.

TABLE 5. The BCR between the original watermark and extracted watermark against some attacks.

Attack	Baboon		Lena	
	PSHT domain	DCT domain	PSHT domain	DCT domain
JPEG compression	87.2	86.9	86.8	85.9
Additive noise	86.4	85.6	85.9	85.1
Histogram equalization	79.4	78.6	78.6	78.1
High pass filtering	82.6	81.9	81.7	80.4
Scaling	87.5	87.3	87.8	87.6

To demonstrate and compare the robustness of our algorithm, the experiments are performed on Baboon and Lena images on DCT domain. Tab.5 gives numerical results

of these experiments. We could conclude that the proposed scheme preserves a good robustness against mentioned attacks.

Although only the Baboon and Lena images have been used as the host images in the tests performed here, the newly presented watermarking scheme has been implemented robustly in a wide range of host images. All aforementioned results suggest that the adaptive proposed method would be 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 can only be embedded into I component. Finally, the embedded image can be obtained by converting the watermarked HIS model into RGB model. Another important issue that was not addressed in this paper is the security of our technique. If the security of watermarking scheme is important, the user can apply the transform parameters as private keys of the algorithm. If the attackers use the parameters that are not the same as the embedding process, the watermark is not extracted properly[40].

7. Conclusion. In this paper, an adaptive scheme for digital image watermarking using parametric slant-Hadamard transform is presented. Traditional transforms such as DCT have the fixed transform matrix, which causes fixed imperceptibility and robustness. However, the parametric slant-Hadamard transform includes some parameters that are suitable for changing the imperceptibility and robustness of watermarking algorithm. This capability motivates us to use this transform to digital image watermarking. The robustness and imperceptibility as the basic requirements of digital watermarking are contradictory to each other. As the results indicated, the variation of transform parameters causes changes on the robustness and imperceptibility simultaneously. Therefore, selection of transform parameters is an important and difficult task. Because of the non-linearity and complexity of parameters, analytical solution to find the parameters to make a trade off between the imperceptibility and robustness is difficult. We select the transform parameters to increase the robustness against some attacks by tabu search and finally, the imperceptibility is enhanced by fuzzy gradient. Fuzzy gradient is calculated using the basic and two relative gradients of each pixel individually. The fuzzy inference system based on the rules produces a single value as a fuzzy gradient. After embedding, the watermarked image is adapted using the fuzzy gradient to enhance the imperceptibility. Moreover, since the watermark embedding is solely determined by the transform parameters, the malicious extraction of the watermark would not be possible without knowing the proper transform parameters. Thus, this scheme is a key dependent method and makes it more stable, compare with other existing algorithms such as DCT.

Acknowledgment. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

- [1] M. Barni, F. Bartolini, and T. Furon, A general framework for robust watermarking security, *Journal of Signal Processing*, vol. 83, no. 10, pp. 2069-2084, 2003.
- [2] Neubauer, Christian, and J. Herre, Advanced watermarking and its applications, *Proc. of the 109th Audio Engineering Society*, pp. 1-19, 2000.
- [3] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, Attack modelling: towards a second generation watermarking benchmark, *Journal of Signal Processing*, vol. 81, no. 6, pp. 1177-1214, 2001.
- [4] K. C. Liu, and C. H. Chou, Robust and transparent watermarking scheme for colour images, *Journal of IET image processing*, vol. 3, no. 4, pp. 228-242, 2009.
- [5] I. Pitas, A method for signature casting on digital images, *Proc. of International Conference on Image Processing*, pp. 215-218, 1996.

- [6] M. Kutter, F. D. Jordan, and F. Bossen, Digital signature of color images using amplitude modulation, *Proc. of SPIE*, vol. 3022, pp. 518-526, 1997.
- [7] D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, A survey of RST invariant image watermarking algorithms, *Journal of ACM Computer Survey*, vol. 39, no. 2, pp. 1-91, 2007.
- [8] J. ÓRuanaidh, and T. Pun, Rotation, scale and translation invariant digital image watermarking, *Proc. of International Conference on Image Processing*, pp. 536-539, 1997.
- [9] P. Premaratne, and C. Ko, A novel watermark embedding and detection scheme for images in DFT domain, *Proc. of International Conference on Image Processing and Its Applications*, pp. 780-783, 1999.
- [10] M. Suhail, M. Obaidat, Digital watermarking-based DCT and JPEG model, *IEEE Trans. Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640-1647, 2003.
- [11] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, Hiding digital watermarks using multiresolution wavelet transform, *IEEE Trans. Industrial Electronics*, vol. 48, no. 5, pp. 875-882, 2001.
- [12] Y. Wang, J. F. Doherty, and R. E. Van Dyck, A wavelet-based watermarking algorithm for ownership verification of digital images, *IEEE Trans. Image Processing*, vol. 11, no. 2, pp. 77-88, 2002.
- [13] H. Li, S. Wang, W. Song, and Q. Wen, Multiple watermarking using Hadamard transform, *LNCS 3739*, Springer, pp. 767-772, 2005.
- [14] S. P. Maity, and M. K. 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.
- [15] X. Zhao, A. T. S. Ho, H. Treharne, V. Pankajakshan, C. Culnane, and W. Jiang, *Proc. of the 3rd International Conference on International Information Hiding and Multimedia Signal Processing*, pp. 283-286, 2007.
- [16] S. Aгаian, K. Tourshan, and J. Noonan, Parametric slant-Hadamard transforms with applications, *IEEE Signal Processing Letters*, vol. 9, no. 11, pp. 375-377, 2002.
- [17] A. Latif, and F. Rashidi, A watermarking scheme based on the parametric slant-hadamard transform, *Journal of Information Hiding and Multimedia Signal Processing*, vol.2, No. 4, pp. 377-386, 2011.
- [18] A. Latif, A. R. Naghsh-Nilchi, and S. Monadjemi, A parametric slant-Hadamard system for robust image watermarking, *Journal of Circuits, Systems, and Computers*, vol. 19, no. 2, pp. 451-477, 2010.
- [19] F. Marqués, M. Menezes, and J. Ruiz-Hidalgo, How are digital images compressed in the web?, *Applied Signal Processing*, Springer, pp. 265-310, 2009.
- [20] J. Xie, S. Aгаian, and J. Noonan, Digital watermarking in parametric slant transform domain, *Proc. of SPIE*, vol. 6821, pp. 68210C.1-68210C.8, 2008.
- [21] D. ElShafie, N. Kharmah, and R. Ward, Parameter optimization of an embedded watermark using a genetic algorithm, *Proc. of the 3rd International Symposium on Communications, Control and Signal Processing*, pp. 1263-1267, 2008.
- [22] P. Artameeyanant, Image watermarking using adaptive tabu search, *Proc. of ICCAS-SICE*, pp. 1941-1944, 2009.
- [23] A. Zolghadrasli, and S. Rezazadeh, Evaluation of spread spectrum watermarking schemes in the wavelet domain using HVS characteristics, *International Journal of Information Science and Management*, vol. 5, no. 2, pp. 123-139, 2007.
- [24] S. S. Aгаian, K. Tourshan, and J. P. Noonan, Partially signal dependent slant transforms for multi-spectral classification, *Journal of Integrated Computer-Aided Engineering*, vol. 10, no. 1, pp. 23-35, 2003.
- [25] S. Aгаian, K. Tourshan, and J. P. Noonan, Generalized parametric slant-Hadamard transform, *Journal of Signal Processing*, vol. 84, no. 8, pp. 1299-1306, 2004.
- [26] J. T. Yin, W. K. S. Tang, and K. F. Man, A comparison of optimization algorithms for biological neural network identification, *IEEE Trans. Industrial Electronics*, vol. 57, no. 3, pp. 1127-1131, 2010.
- [27] F. Glover, E. Taillard, and D. Werra, A user's guide to tabu search, *Journal of Annals of Operations Research*, vol. 41, no. 1, pp. 1-28, 1993.
- [28] A. T. S. Ho, X. Zhu, Y. L. Guan, and P. Marziliano, Slant transform watermarking for textured images, *Proc. of IEEE international Symposium on Circuits and Systems*, pp. 700-703, 2004.
- [29] H. Qia, D. Zheng, and J. Zhao, Human visual system based adaptive digital image watermarking, *Journal of Signal Processing*, vol. 88, no. 1, pp. 174-188, 2008.
- [30] D. Van De Ville, M. Nachtgael, D. Van der Weken, E. E. Kerre, W. Philips, and I. Lemahieu, Noise reduction by fuzzy image filtering, *IEEE Trans. Fuzzy Systems*, vol. 11, no. 4, pp. 429-436, 2003.
- [31] Y. H. Yu, and C. C. Chang, A new edge detection approach based on image context analysis, *Journal of Image and Vision Computing*, vol. 24, no. 10, pp. 1090-1102, 2006 .

- [32] D. C. Lou, and T. L. Yin, Adaptive digital watermarking using fuzzy logic techniques, *Journal of Optical engineering*, vol. 41, no. 10, pp. 2675-2687, 2002.
- [33] C. Jin, Robust wavelet-domain watermark scheme based on fuzzy technology, *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems*, vol. 15, no. 6, pp. 737-751, 2007.
- [34] C. T. Leondes, *Fuzzy theory systems: techniques and applications*, Academic Press, Los Angeles, U.S.A., 1999.
- [35] H. Ying, Y. Ding, S. Li, and S. Shao, Comparison of necessary conditions for typical takagi-sugeno and mamdani fuzzy systems as universal approximators, *IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 29, no. 5, pp. 508-514, 1999.
- [36] F. A.P. Petitcolas, Watermarking schemes evaluation, *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 58-64, 2000.
- [37] S. C. Chu, H. C. Huang, Y. Shi, S. Y. Wu, and C. S. Shieh, Genetic watermarking for zerotree-based applications, *Journal of Circuits, Systems, and Signal Processing*, vol. 27, no. 2, pp. 171-182, 2008.
- [38] M. Xenos, K. Hantzara, E. Mitsou, and I. Kostopoulos, A model for the assessment of watermark quality with regard to fidelity, *Journal of Visual Communication and Image Representation*, vol. 16, no. 6, pp. 621-642, 2005.
- [39] G. K. Wallace, The JPEG still picture compression standard, *Journal of Communications of the ACM*, vol. 34, no. 4, pp. 30-44, 1991.
- [40] W. Dietl, P. Meerwald, and A. Uhl, Protection of wavelet-based watermarking systems using filter parametrization, *Journal of Signal Processing*, vol. 83, no. 10, pp. 2095-2116, 2003.