Multimed Tools Appl (2011) 52:347–367
DOI 10.1007/s11042-010-0475-5

Wavelet tree based digital image watermarking by adopting the chaotic system for security enhancement

Min-Jen Tsai

Published online: 9 February 2010

Abstract Wavelet tree based watermarking algorithms are generally using the wavelet coefficient energy difference for copyright protection and ownership verification. Since there are cryptanalysis-based methods addressed for successfully attacking wavelet tree based watermarking algorithm of wavelet tree quantization (WTQ), it is the motivation in this research to devise a scheme to improve WTQ's robustness. Furthermore, the combination of wavelet tree based watermarking techniques, chaotic system for block based scrambling techniques have not been seen or few discussed in the literatures. The study in this paper has presented such research findings and contribution for the academic and industry fields. Therefore, a chaotic system is adopted for WTQ to counteract the attacks in this paper. The digital image is first split into many blocks and the chaotic system is applied to scramble the image before the implementation of WTQ. The experimental results demonstrate the effectiveness of using chaotic system to enhance the security of WTQ, especially, to resist cryptanalysis attack. In addition, such mechanism also works for other advanced wavelet tree based algorithms like wavelet tree group modulation (WTGM) and dynamic energy enabled differentiation (called DEED) watermarking techniques.

Keywords Chaotic system · Wavelet-tree quantization

1 Introduction

Digital media files can be easily copied and distributed without any reduction in quality. Piracy is a concern when security measures are not in place to protect content. Conventional cryptographic systems permit only valid principals (key holders) access to encrypted data. Once such digital data are decrypted, there is no way to track their reproductions or retransmissions. Over the last decade, digital watermarking has been presented to complement cryptographic protection mechanisms.

M.-J. Tsai (✉)
National Chiao Tung University, Hsinchu, Taiwan, Republic of China
e-mail: mjtsai@cc.nctu.edu.tw

Cox et al. [3] proposed a global DCT-based spread spectrum approach to hide watermarks. The frequency domain of the image or sound is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. The watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. Langelaar and Lagendijk [11] introduced the DEW (Differential Energy Watermarking) algorithm for JPEG/MPEG streams in the DCT domain. The DEW algorithm embeds label bits (the watermark) by selectively discarding high frequency DCT coefficients in certain image regions. Wang and Lin [10, 24] introduced the philosophy of WTQ (Wavelet Tree Quantization) in the DWT domain. The wavelet coefficients are grouped into so-called super trees. The wavelet-tree-based watermarking algorithm embeds watermark bits by selectively quantizing super trees. Even if the attacker has no knowledge of which two trees are used for embedding, he can still quantize those super trees that are not quantized earlier with respect to the estimated quantization indices. Das and Maitra had presented how that can be accomplished in [4] and such cryptanalysis attack is also confirmed in this study.

Instead of only using the tree structure in the wavelet domain for image watermarking, tree group energy differentiation approach with the adoption of human visual system has been first proposed in WTGM [19, 20] algorithm. In WTGM, suppose that each watermark bit is embedded using one tree group, half of a tree group is used for positive modulation [12] and the other is used for negative modulation. For suitable modulation, any two sub-tree groups should have close total energy (energy summation from wavelet tree coefficients) and the selection is essential the sum-of-subset problem in [5].

On the other hand, it is also possible to apply the dynamic energy enabled differentiation to investigate the differentiation approach with human visual system consideration for watermarking [18]. Under such conception, [18] proposed a human vision system based dynamic energy enabled differentiation (called DEED) watermarking algorithm which utilizes discrete wavelet transform (DWT) theory. DEED modifies the wavelet coefficient values of images dynamically and uses the differentiation of positive and negative modulation to embed the watermark. In the embedding process, [18] tries to find the best coefficient energy differentiation direction of the embedded watermark bit that make minimal change of coefficient's energy within the tree. It then changes the wavelet tree coefficient energy dynamically with differentiation direction, and embeds the designated watermark bits into the energy differentiation between the coefficients. The purpose of the DEED design is robust to the cryptanalysis of the watermarking attacks with high visual quality.

Whether the security of watermarking algorithms can be preserved, if the details about algorithms are released, it is the "Security by Obscurity" (the assumption that opponent will remain ignorant about the system being used) issue which the cryptographic principle was first introduced by Kerckohoffs [8] in 1883. Therefore, the watermarking algorithm will be known to the attacker as it is accepted in the field of cryptology [4, 7].

Taking a birds eye view on cryptography [7], there is a single prominent property that makes encryption a good security tool, viz. its extreme sensitivity to bit changes. More concretely, if a message **M** is encrypted with some encryption protocol **E** and key **K**, $\mathbf{M_E} = \mathbf{E_K}[\mathbf{M}]$, then a single bit change in either the key **K** or the message **M** will result in a completely different encrypted message $\mathbf{M_E}$.

Formulated in more topological terms we observe that a good encryption method (as well as the corresponding decryption method) is highly discontinuous with respect to Hamming distance. A well-designed encryption scheme is not only highly discontinuous for the Hamming topology, but also for any other topology. In fact, again with a birds eye view, one could say that a large part of the research on cryptoanalysis is concerned with finding topologies on message space such that encryption and decryption functions have a more continuous character. If such a structure can be found, it usually dramatically reduces the effort needed for unauthorized decryption. One of the fundamental problems addressed in crypto-analysis is the recovery of an original message **M** from an encrypted message $\mathbf{M_E}$: the (symmetric) encryption method E is assumed to be known, but not so the encryption key **K**. Ideally, for a well-designed encryption method, the only option for an attacker is an exhaustive search of the key space. The key property that forces such an exhaustive search is that an attacker should obtain only minimal information from trying: an experiment with a key **K** that fails, should give no more information than that key **K** is the wrong key. Not a single bit of information on any of the other keys should become available!

The above fundamental problem in cryptography has a direct analogy in the field of watermarking. In the case of watermarking, the objective of the attack is either to learn the watermarking key **K** from a watermarked object $\mathbf{O_w}$, or to estimate an unmarked object $\mathbf{O_u}$ that is perceptually similar to the original object **O**. In all this we of course assume that the watermarking method **W** is known (Kerckhoffs' principle [8]). The difference with cryptographic systems is that in general for watermarking there is a *continuous dependency* of detector decision values on the *pseudo-random sequences encoded by the key and message*. Without this continuity property it is impossible to build a robust watermarking system: the slightest degradation of a watermarked object would make the watermark unreadable. As is well known from basic mathematics and cryptography, continuous functions are easier to analyze than chaotic function: any observation for a given set of input parameters yields information on similar input parameters. This observation is in fact the philosophical basis of the sensitivity attack proposed in [2]. Therefore, it is also the motivation in this study to apply the chaotic system for the watermarking since the chaotic system can enhance the security level of the watermarking through above analysis.

In this paper, we first briefly explain the WTQ scheme and the cryptanalysis attack in Section 2 and then devise how to improve its robustness by applying the chaotic system as a pre-processing mechanism in Section 3. The experimental results are demonstrated in Section 4 with further discussion is in Section 5, and the conclusion is in Section 6, respectively.

2 WTQ scheme

The WTQ scheme is a wavelet tree based blind watermarking scheme. Interested reader can refer reference [24] for detailed information and we briefly explain the operations:

2.1 Group the super tree

In the WTQ scheme, a pair of super trees is used to record one watermark bit, and the watermark is a binary PN sequence of {1, −1}. Before recording all watermark bits, we should perform 4-level DWT as shown in Fig. 1(a), and collocate coefficients in $C_{i,j}$, where i={2, 3, 4} and j={1, 2, 3}, to form the groups in Fig. 1(b). A group has 21 coefficients: 1 coefficient from level-4, 4 coefficients from level-3, and 16 coefficients from level-2. After grouping, two groups are randomly combined to become a super tree and there are 42 coefficients in every super tree.

While all super trees are grouped, WTQ starts to embed the watermark bits by quantization. Here we pair two super trees with a secret seed for quantization operation, so

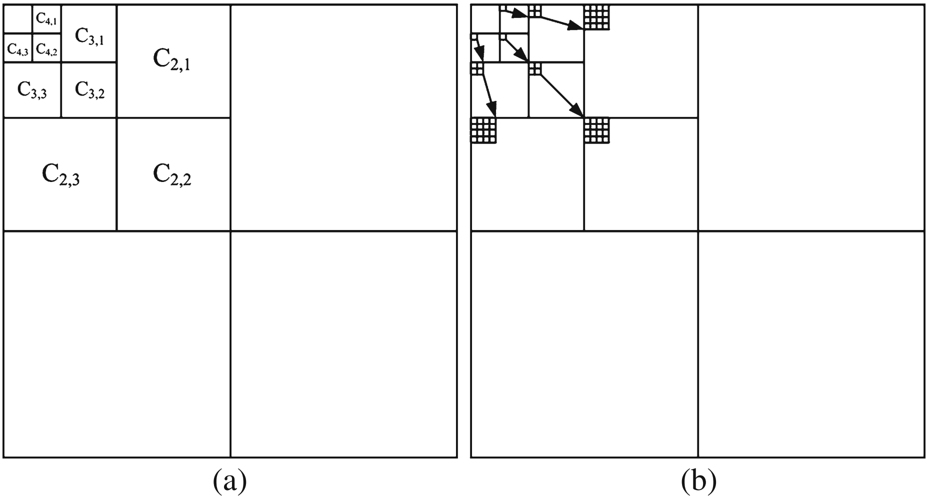


Fig. 1 **a** Pyramidal wavelet decomposition. **b** Three sample groups

one super tree of a pair will be quantized for recording the information of the corresponding watermark bit. For example, if the current watermark bit is 1, we will quantize the left super tree in the corresponding pair. Otherwise, the right one will be quantized.

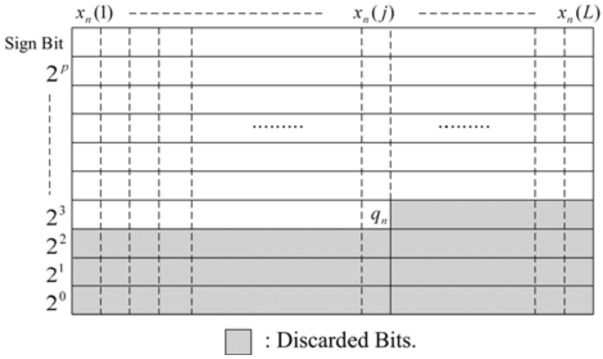
In order to perform quantization, all super trees will be transformed to "bit-plane" form first.

2.2 Form the bit-plane for quantization

A super tree will be transformed to the bit-plane format as shown in Fig. 2 for calculating the scope of bits which will be selectively removed according to the reference error. In Fig. 2, the energy of the gray area is the same with or bigger than the reference error. When we have found the scope, bits in the gray area will be discarded.

In WTQ, every watermark bit is recorded with a tree-pair. If we want to extract the watermark, both trees in a tree-pair will be checked and than we will find out which tree is quantized. Thus, according to the quantization pattern, we can get the information of the current watermark bit. To quantify the existence of the watermark, the normalized

Fig. 2 Bit-plane form and quantization Area



correlation coefficient [24] will be examined in order to identify the existence of the watermark. The formula of normalized correlation coefficient is as follows:

$$\rho(W, W') = \frac{\sum_{m=1}^{N_w} w_m w'_m}{N_w} \tag{1}$$

The coefficient value is within −1 and 1. The existence decision is "yes" if $\rho(W,W') \geq \rho_T$ and "no" if $\rho(W,W') < \rho_T$. The threshold ρ_T is chosen based on the probability of false positive error P_{fP} which is computed by [24]:

$$P_{fP} = \sum_{n=\lceil N_w \times (\rho_T+1)/2 \rceil}^{N_w} \binom{N_w}{n} P_E^{N_w-n} \cdot (1-P_E)^n \tag{2}$$

The estimation of the probability of a false positive (i.e., false watermark detection) is analyzed as following [10]:

We define the probability of false watermark detection as

$$P_{fp} = P\left\{\rho\left(W, \widetilde{W}\right) \geq \rho_T \middle| \text{no watermark}\right\} \tag{3}$$

where $P\{\mathrm{A}|\mathrm{B}\}$is the probability of event A given event B, W is the given watermark and $\widetilde{W}$ is the extracted one. Since $W(n)$ and $\widetilde{W}(n)$ are either one or negative one, and subsequently $W^2(n) = \widetilde{W}^2(n) = 1$. Let P_E be the probability of bit error during extraction. A bit error occurs when $\widetilde{W}(n) \neq W(n)$ or more specifically, when $\widetilde{W}(n) = -W(n)$ (since $W(n), \widetilde{W}(n) \in \{-1, 1\}$). If we let $k(n) = W(n) \cdot \widetilde{W}(n)$, then $k(n)=-1$ indicates a bit error and $k(n)=1$ indicates no error. We may rewrite the expressions for ρ and P_{fp} in terms of $k(n)$ as

$$\rho\left(W, \widetilde{W}\right) = \frac{\sum_{n=1}^{N_w} W(n)\widetilde{W}(n)}{N_w} = \frac{\sum_{n=1}^{N_w} k(n)}{N_w} \tag{4}$$

and

$$P_{fp} = P\left\{\sum_{n=1}^{N_W} k(n) \geq N_w \rho_T \middle| \text{no watermark}\right\}, \tag{5}$$

Since $k(n) \in \{-1, 1\}$, it can be shown that $\sum k(n)$ must take on discrete values from the set $\{-N_w, -N_w+2, -N_w+4, \ldots, N_w-4, N_w-4, N_w-2, N_w\}$, or $\sum k(n) = -N_w + 2m$, where m=0,1,..., N_w. Thus, we find that

$$\begin{aligned} P_{fp} &= P\left\{\sum_{n=1}^{N_W} k(n) \geq N_w \rho_T \middle| \text{no watermark}\right\} \\ &= \sum_{m=\lceil N_w(\rho_T+1)/2 \rceil}^{N_W} P\{\textstyle\sum k(n) = -N_w + 2m | \text{no watermark}\}, \end{aligned} \tag{6}$$

Where $P\{\sum k(n) = -N_w + 2m \,|\, \text{no watermark}\}$ is the probability that the series $\{k(n)\}$ contains m ones and N_w–m negative ones. Since $\sum k(n) = -N_w + 2m \geq N_w \rho_T$ and $2m \geq N_w \rho_T + N_w$, m's range is from $\lceil N_w(\rho_T+1)/2 \rceil$ to N_w. Therefore,

$$P\left\{\sum k(n) = -N_w + 2m \middle| \text{no watermark}\right\} = \binom{N_w}{m} P_E^{N_w-m} \cdot (1-P_E)^m \tag{7}$$

Where P_E is the probability that $k(n)$=−1 and $\begin{pmatrix} N_w \\ m \end{pmatrix} = \frac{N_w!}{m!(N_w-m)!}$. Since we are given that no watermark is embedded, we can assume that extracted mark $\widetilde{W}$ consists of a series of random independent equally probable values from the set $\{-1,1\}$. Thus, P_E=0.5. Substituting into Eqs. 6 and 7,

$$P_{fp} = \sum_{m=\lceil N_w(\rho_T+1)/2 \rceil}^{N_W} \begin{pmatrix} N_w \\ m \end{pmatrix} 0.5^{N_w}. \tag{8}$$

Given the reasonable assumption, P_E=0.5 and N_w=512 as the watermark length, P_{fp} will be as low as 4.5×10^{-1}, 3.86×10^{-1} and 8.45×10^{-9} while ρ_T=0.15, 0.20 and 0.25 respectively. That means the appropriate ρ_T will be selected to meet the requirement given a false positive probability.

2.2.1 Cryptanalysis attack for WTQ

In [4], Das and Maitra claimed that every existing watermarking algorithm should be tested as a cryptographic model by cryptanalysis. Therefore, Das and Maitra put the cryptanalytic techniques on the WTQ scheme, and found out the weakness. As the paper says, “knowledge of groups, which is image dependent, but not dependent on secret seed, is enough for successful removal of correlation.” Although the information of constructing a super tree is unknown, but we know that every super tree is obtained with two groups. In order to destroy the watermarking information in super tree, we can use indirect technique through the knowledge of groups.

The cryptanalysis on WTQ can be divided into three steps: identification of quantized and non-quantized groups, estimate of reference error, and quantization of non-quantized groups.

1. Identification of quantized and non-quantized groups

All groups will be transformed into bit-plane format for identification. The principle is calculating the energy of last rows. If the bits of last rows in current group are almost empty, we can assume this group as a quantized group. Otherwise, this group is a non-quantized group.

2. Estimation of reference error

After identification, we take the set of quantized groups for estimation. First, we calculate the quantization error of all groups in the set, and find out that the energy removed in every group is almost ε'. Thus, ε' is the estimated reference error.

3. Quantization of non-quantized groups

When reference error has been estimated, the set of non-quantized groups will be quantized using this estimated reference error. After this step, all groups are almost quantized.

In WTQ, every watermark bit is recorded by quantizing only one tree in a pair. Making all groups quantized means making all super trees quantized because a super tree is merged with two groups. Thus, if all trees are quantized, the difference caused by quantization between two trees in a pair will be eliminated. As the difference between both trees declines, it is difficult for the detector to extract the watermark bit accurately.

3 Chaotic systems

In steganalysis, the message hidden in a cover image will be detected easily by attackers, if there is no protection. In order to enhance the security, the image scrambling is exploited. As a kind of security mechanism in steganalysis, when the secret message has been hidden, image scrambling is adopted to disorder the cover image before transferring it into the public network.

Compared to original image, a scrambled image is more robust under the detection of attackers which is one of the applications of chaotic system. We can see the scrambled image as a different image from original one. Besides, when an image was split to many sub-images through scrambling, the capacity of the watermark in every sub-image is not enough for detection. Thus, the scrambled image will escape from the monitor of the web-crawling detector. Scrambling is like a kind of encryption. When we scramble an image with a secret seed, the scrambled image is just like another image. If someone doesn't know the secret seed, it is difficult for the receiver to reconstruct the scrambled image and extract the watermark correctly.

Therefore, this study will use a chaos-based watermarking to improve its security. Before watermark embedding, the host image will be scrambled first. The flowchart of scrambling by the chaotic system is shown in Fig. 3. There are two primary variables for image chaotic system: "the algorithm of chaotic system" and "image split size". Before our discussion of security improvement by image scrambling, the setting of these two variables will be discussed first.

3.1 Chaotic system algorithms

Even there are many pseudo random sequence generators can be used to generate pseudo random sequence that used to scramble the image, the author has tried many different random sequences for scrambling and selected the best performance from different chaotic system including random ordering, Fibonacci transformation and Toral Automorphism. An example of scrambled images by different chaotic system is illustrated in Fig. 4. The random ordering is like card shuffling. Fibonacci transformation is adopted from [1, 25], and the formula is

$$S_k = (kF_n + r) \bmod F_{n+1}, k = 0, 1, 2, \ldots\ldots, F_{n+1} - 1, \tag{9}$$

F_n and F_{n+1} are both Fibonacci numbers and k is the array of original order. The constraint is that the length of ordering array should be a Fibonacci number. Thus, we will randomly insert some extra value into the array to make the length as a Fibonacci number. When scrambling has finished, these extra values will be removed.

Toral Automorpism [21, 23] is generally used in two dimensional array. The formula is

$$A_N(k) : \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N) \tag{10}$$

Where k is a control argument decided by the user. N is the size of array, (x, y) and (x', y') is the pixel location before and after the transform. Since Toral Automorphism has a recurrence time, after some times of transformation, the array will return to original order. The recurrence time is irregular, but it changes as k or N changed. Because Toral Automorphism has a recurrence time, even the attacker using a different secret seed, the scrambled image may be the same. Thus, Toral Automorphism is not secure enough in practice.

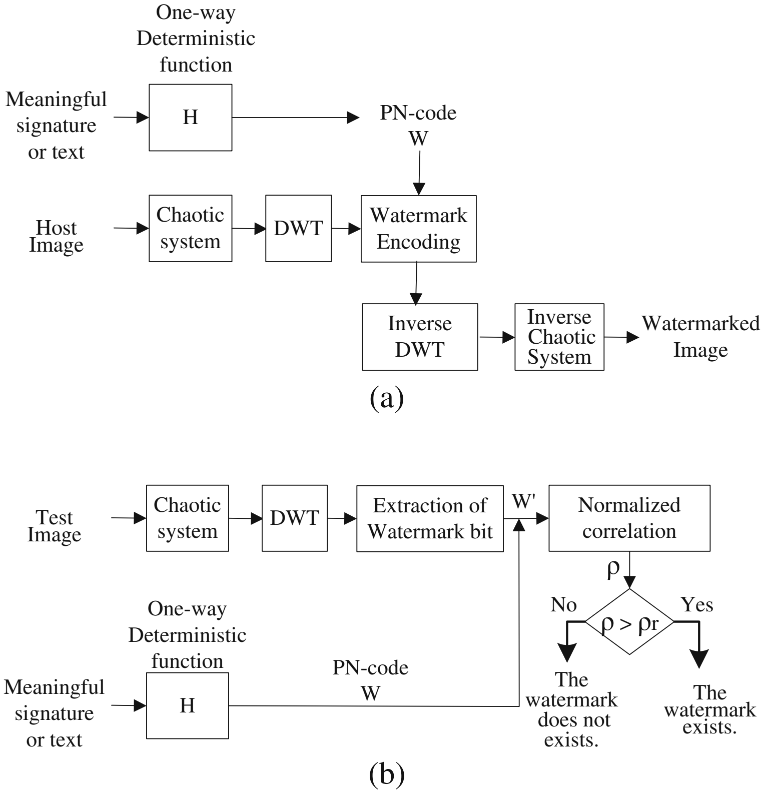
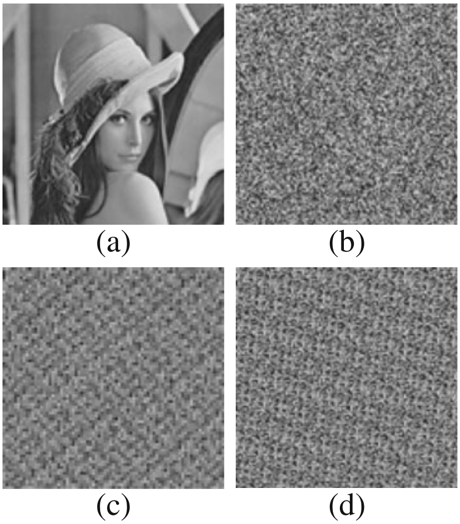


Fig. 3 The process of chaotic system module applied in (**a**) watermark embedding and (**b**) extraction flow charts

Fig. 4 Image scrambled by (**a**) no scrambling (**b**) random scrambling (**c**) Fibonacci (**d**) Toral automorphism chaotic system



Random ordering and Fibonacci transformation are both secure after further investigation. However, Fibonacci transformation is more secure because “it separates adjacent pixels as far as possible from each other”[25]. Thus, Fibonacci transformation could be the most applicable chaotic system for common use and it will be applied in the study.

3.2 Image split size for the chaotic system

Before applying the chaotic system, the image will be split into many blocks. For example, if we set the split size as 4, the image will be split into many 4×4 blocks before applying the chaotic system. Otherwise, if the split size is 1, the image will be scrambled based on the unit of per pixel.

The smaller the split size is, the larger the number of blocks will be. Take a 512×512 gray-level image for example, if the split size is 4, there are going to have 16384 blocks. It means there will be 16384!(about 10^{61936}) permutation for scrambling. When we set the split size as 8, the number of permutation will be 4096!. Thus, the smaller the split size is, the more secure the scrambling operation is.

However, when the split size is reduced, the scrambling operation will decrease the robustness of watermarking. The influence of split size on the robustness of watermarking under JPEG compression attack is in Fig. 5 for 512×512 Lena image. Therefore, we found that the split size properly enlarges, the robustness also increases. The security will be better when the split size is smaller, but the watermark will be more robust when the split size is larger. In order to get a balance, we choose the split size at 4×4 as our setting for chaotic system in this study. Besides of Lena, we also test other images like Goldhill and Peppers which also give us the similar results.

4 Security experiments

The effective influence of chaotic system on the robustness of watermarking needs to be evaluated. To make fair comparison, three wavelet-tree-based watermarking algorithms are adopted here for experiments and comparison for the test of robustness with and without

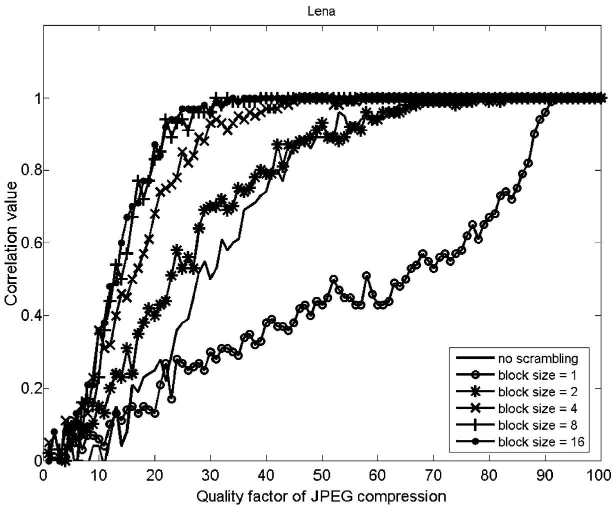


Fig. 5 The plots of correlation value v. s. JPEG quality factor for Lena under different split block size

using the chaotic system mechanism. These three watermarking scheme are WTQ of [24], WTGM [19, 20], and DEED [18]. Interested readers could refer the reference for detailed information.

Because these schemes are not the same, in order to make the fair comparison, all the same testing watermarked images will be set at the same PSNR values as described in [24]. During our simulation, the PSNR values of watermarked images are 38.2, 38.7, and 39.8dB respectively for Lena, Goldhill and Peppers. The correlation threshold ρ_T is chosen to be 0.23 for a false positive probability P_{fp} of 1.03×10^{-7} given N_w=512 in order to have the performance comparison with data in [24]. Some results are explained in details as follows:

4.1 Geometric and nongeometric processing

Within Table 1, several geometric and nongeometric processing attacks are tabulated for WTQ and WTQ(s) while WTQ(s) means the collaboration of WTQ with the chaotic system. The attacks are listed as following: Attack(**A**) is the median filter attack with mask size of 4×4 and Attack(**B**) is the median filter attack with mask size of 5×5. Two types of pixel shifting of 9 pixels are for attack(**C**) and (**D**). Attack(**C**) is a circular shift operation and attack (**D**) is a deletion of lines followed by duplication of the adjacent lines. Attack(**E**) is 4 least significant bitplanes removal from the wavelet coefficients in the transform domain. Attack(**F**) is 4 multiple watermarking attack. The rotation and scaling attack is for (**G**) of -0.75 degree and (**H**) of 1 degree. Attack(**I**) is Gaussian filtering and attack(**J**) is sharpening attack. Attack(**k**) is the cryptanalysis attack from [4] while the total reference error is set at 150.

From Table 1, all correlation values under WTQ(s) the proposed approach are higher than the threshold of 0.23 but data from [3] of WTQ from [24] are not all above the threshold. Especially, WTQ(s) can resist the cryptanalysis based attack. To further explain the cryptanalysis attack of (K), following section will describe its approach and its detailed experimental results.

According to our simulation of the cryptanalysis attack for WTQ, the unquantized bitplane could be successfully identified and the last two rows could be removed.

Table 1 Comparison of WTQ and WTQ(s) under geometric and nogeometric processing attacks

Method	WTQ			WTQ(s)		
Attack	Lena	Peppers	Goldhill	Lena	Peppers	Goldhill
(A)	0.23	0.24	0.35	0.40	0.34	0.36
(B)	NA	NA	NA	0.42	0.35	0.43
(C)	0.26	0.29	0.29	0.27	0.36	0.37
(D)	0.25	0.25	0.28	0.28	0.26	0.31
(E)	0.52	0.38	0.64	0.63	0.58	0.73
(F)	0.11	0.18	0.22	0.24	0.30	0.26
(G)	0.24	0.25	0.25	0.29	0.38	0.33
(H)	0.24	0.15	0.17	0.27	0.26	0.28
(I)	0.64	0.56	0.74	0.89	0.93	0.92
(J)	0.46	0.39	0.62	0.88	0.63	0.90
(K)	0.0	0.0	0.0	0.58	0.55	0.57

Therefore, the watermark will be removed even without the reference error estimation. As the difference between both trees reduced, it is difficult for the detector to extract the watermark bit accurately. Therefore, WTQ is not secure enough for digital watermarking in principle. However, all the correlation values of the chaotic system based watermarking images are above the threshold 0.23 while the reference error increases in Fig. 6 which means they can successfully resist the cryptanalysis based attack.

From extensive experimental study of WTGM and DEED for geometric and nongeometric, cryptanalysis attacks, similar performance are obtained. Without tabulating all the attacks for WTGM and DEED in this paper, it is evident the collaboration of chaotic system can efficiently improve the robustness against the attacks, especially, to resist the cryptanalysis based attack for wavelet tree based watermarking algorithms.

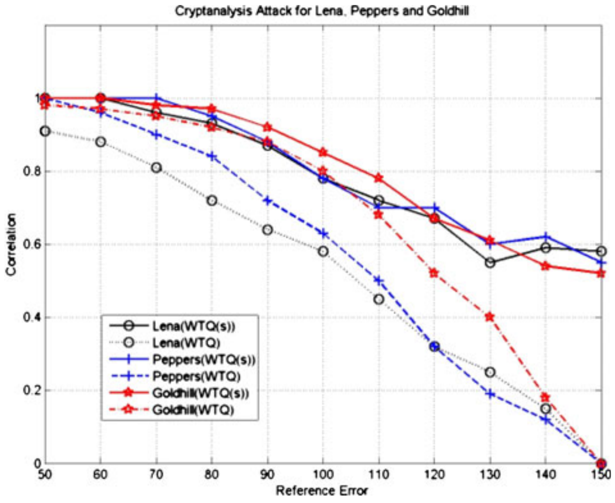
4.2 JPEG compression

JPEG Compression is a common frequency-domain based attack. In Fig. 7, the horizontal axis is the quality factor of JPEG compression. As the value is smaller, the degradation of image is more obvious. While the quality factor is at 20, the results of WTQ(s) can be all above the threshold but the results of WTQ are not. From Fig. 7, it is obvious that the chaotic system significantly improves the robustness of WTQ. Even the improvement of chaotic system for WTGM and DEED is not as apparent as WTQ, the correlation values are higher while the chaotic system is applied for all three algorithms of WTQ, WTGM and DEED for JPEG compression attack.

4.3 SPIHT compression

SPIHT (Set Partitioning in Hierarchical Trees) [16] is an image compression algorithm that exploits the inherent similarities across subbands in a wavelet decomposition of an image. It implies uniform quantization and bit allocation applied after wavelet decomposition. Similar to the results in Fig. 7, the correlation values in Fig. 8 are higher while the chaotic system is applied for all algorithms.

Fig. 6 Cryptanalysis attack of WTQ and WTQ(s) for Lena, Peppers and Goldhill images. (s) means the chaotic system is applied



4.4 Median filtering

The median filter is normally used to reduce noise in the image. With median filtering, the value of an output pixel is determined by the median of the neighborhood pixels.

The results of median filtering of Fig. 9 with chaotic system are also useful for WTQ, WTGM and DEED algorithms.

4.5 Rotation and scaling

The attack is done by rotating the image by a small angle, scaling the rotated image, and cropping the scaled image to the original image size. StirMark [17] software is adopted here for this attack since it provides the described testing functions. This rotation and scaling is a geometrical attack in the spatial domain. In Fig. 10, the value of horizontal axis is the degree of rotation. The result of robustness is also enhanced for all WTQ, WTGM and DEED algorithms.

As the results of Figs. 7, 8, 9 and 10, the robustness of watermarking with chaotic system performs better for all schemes under geometric and non-geometric attacks. Since the wavelet coefficients are scrambled and reordered, the cryptanalysis-like attack will no longer be valid to remove the watermark. Therefore, the security robustness is enhanced under the chaotic system.

5 Discussion

From the simulation results in Section 4, it is apparent that applying the chaotic system for wavelet tree based watermarking algorithms could enhance the security robustness. Therefore, it is essential to analyze the characteristics of the original images and the images under chaotic system by using the statistical features in order to understand which image features could be the important indicators for using the chaotic system.

In this study, we have exploited wide variety of statistical features for analysis of the image features including energy, entropy, image activity measure (IAM), kurtosis, log energy entropy, range, shannon entropy, skewness and variance, ...etc. Through the results of these features, we have found out that energy, kurtosis and log energy entropy can be the indicators among others for explaining how chaotic system improves the security for the wavelet based watermarking algorithms since their simulation results shows consistent regularity than others. Table 2 lists all three feature formulas, where $I(i)$ is the image intensity value of pixel i.

For actually reflecting the influence of chaotic system on the robustness of these wavelet-tree-based watermarking algorithms, 4-level wavelet decomposition is performed first to get the associated 9 subband feature values as shown in Fig. 8 since the discussed wavelet tree based algorithm of WTQ, WTGM and DEED only use those 9 bands to embed watermarks. To thoroughly examine the statistical features, there are total 12 widely used images from [22] are tested under this simulation and those images are shown in Figs. 11 and 12.

The results of the three features are in Figs. 13, 14 and 15, where the feature in each subband is plotted for comparison. Each feature of 9 subbands for 12 testing images are averaged and drawn together while (1) is the original image (2) is the image applied by random ordering (3) is the image scrambled by Fibonacci transformation and (4) is the image applied by Toral Automorphism.

Fig. 7 The plots of correlation value v.s. JPEG quality factor for watermarked Lena, Goldhill and Peppers images. Three images are watermarked by WTQ, WTGM and DEED algorithms. (s) means the algorithm is applied by the chaotic system. Threshold is marked by the dark red line

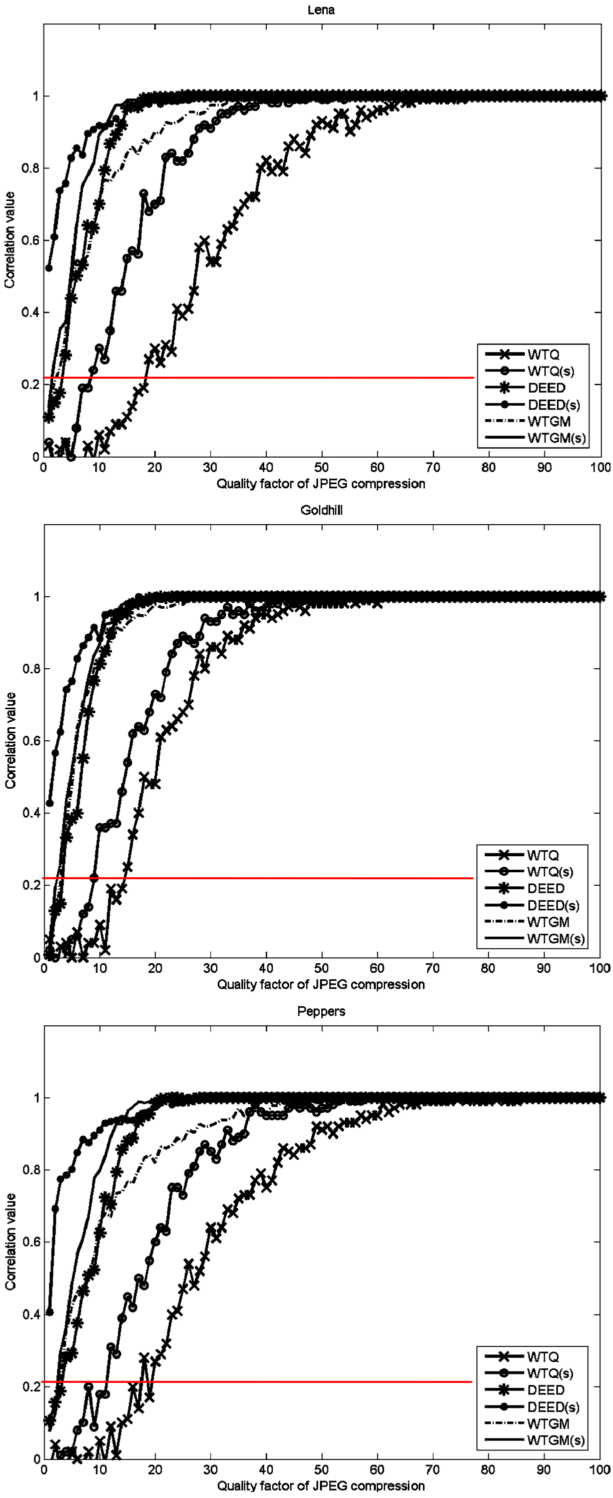
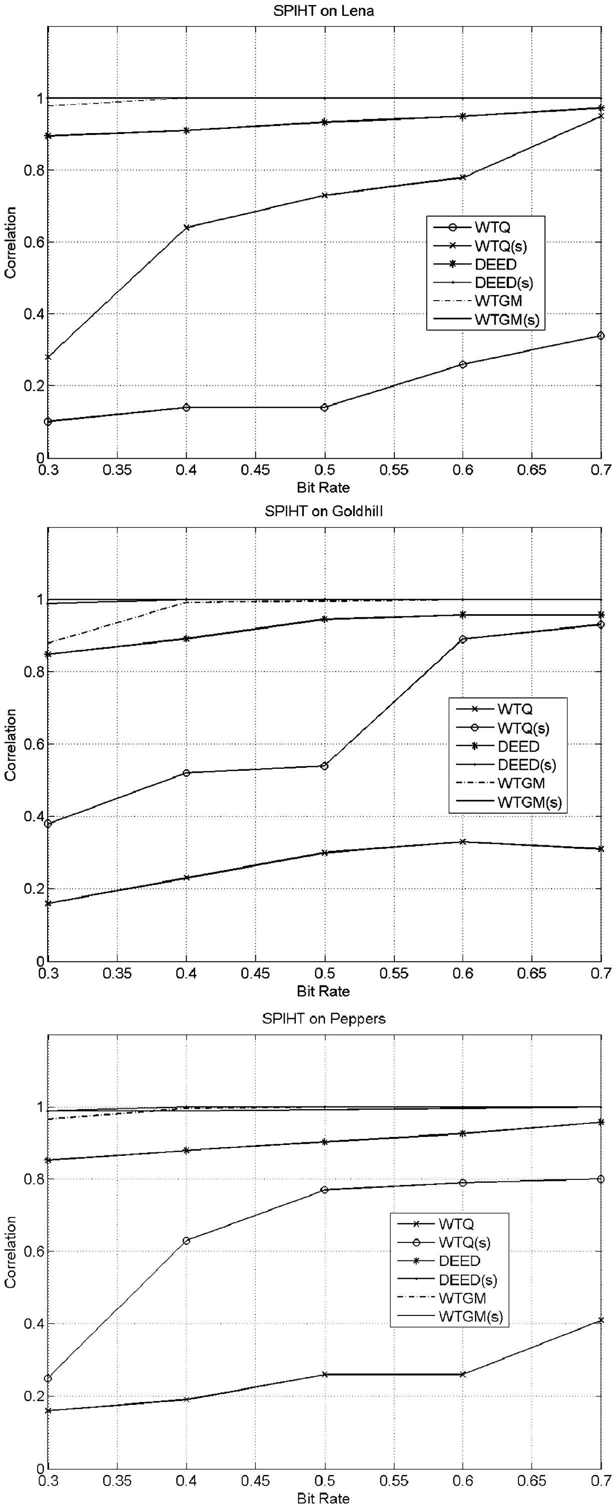


Fig. 8 The plots of correlation value v. s. SPIHT compression ratio for Lena, Goldhill and Peppers images. Three images are watermarked by WTQ, DEED and WTGM algorithms. (s) means the algorithm is applied by the chaotic system



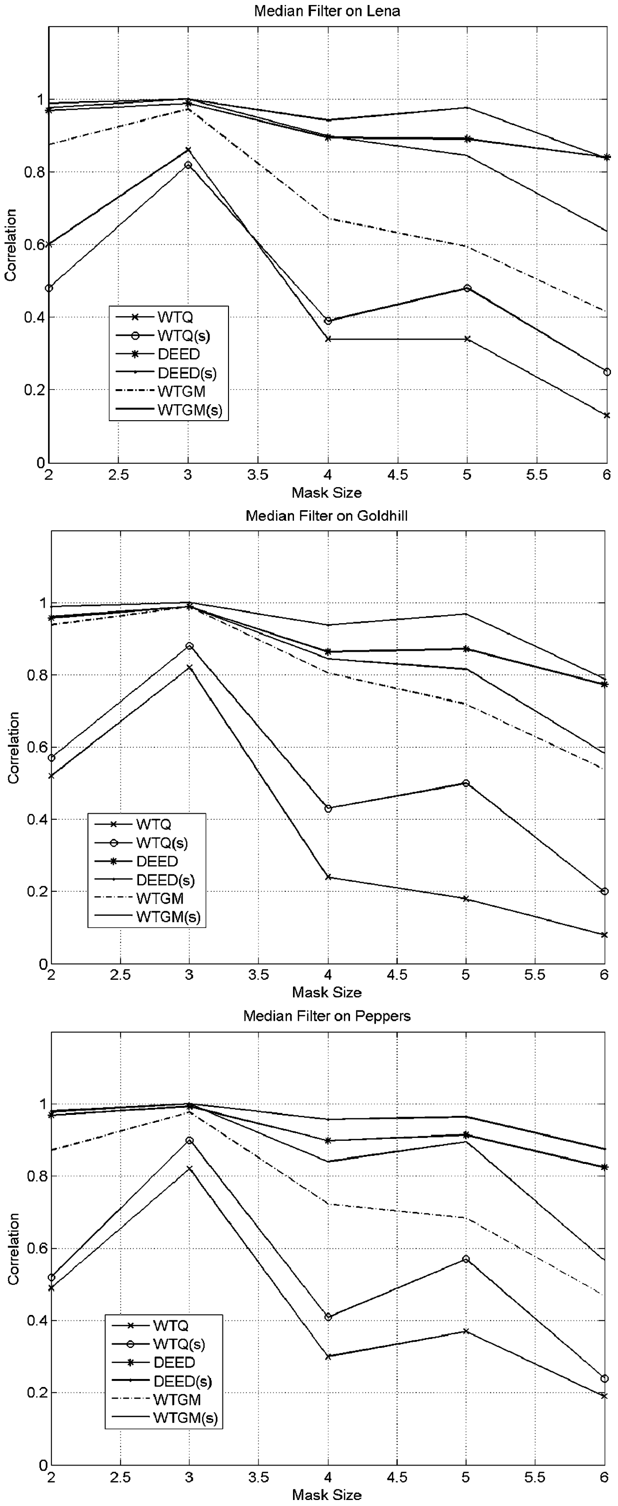


Fig. 9 The plots of correlation value v. s. median filtering for Lena, Goldhill and Peppers images. Three images are watermarked by WTQ, DEED and WTGM algorithms. (s) means the algorithm is applied by the chaotic system.

Fig. 10 The plots of correlation value v. s. rotation and scaling for Lena, Goldhill and Peppers images. Three images are watermarked by WTQ, DEED and WTGM algorithms. (s) means the algorithm is applied by the chaotic system

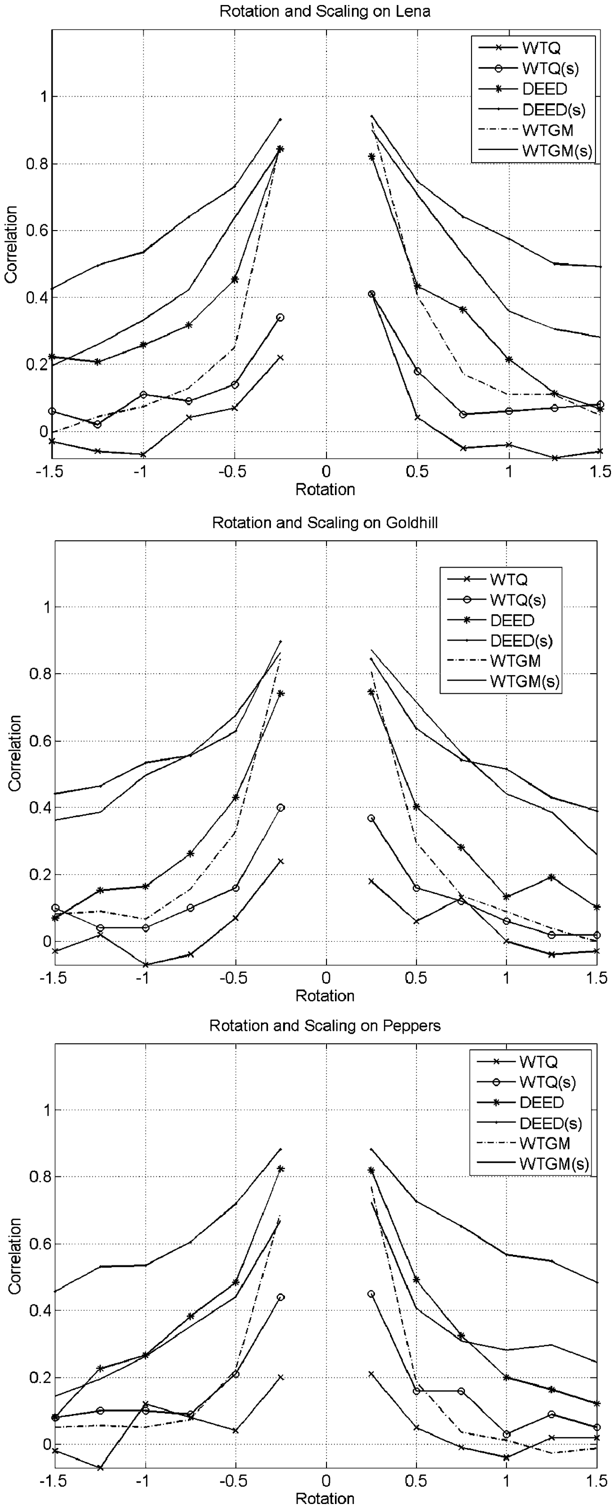


Table 2 The statistical features

Feature	Formula
Energy	$E = \frac{1}{N}\sum_i I(i)^2$
Kurtosis	$k = \frac{1}{N}\sum_i \left(\frac{I(i)-m}{\sigma}\right)^4 - 3$
Log Energy Entropy	$E_{le} = -\frac{1}{N}\sum_i \log\left(I(i)^2\right)$

The effectiveness of different chaotic systems for the wavelet tree based watermarking system is different through the extensive experiments in this study. It is important to apply the appropriate chaotic system for the applications.

In the result of energy in Fig. 13, the energy in original image almost locates at low-frequency (bands 1–3). After applied by chaotic system, the energy in band 4–8 will be significantly increased. When the energy in middle-frequency is enlarged, there will be more capacities for embedding the watermark. Since many watermarking algorithms use middle-to-high frequency bands to embed the watermark, if the capacity increases, the robustness will be enhanced.

The kurtosis in Fig. 14 for all 12 images reflects the distribution of pixels. When the value is close to zero, the distribution of pixels is more like a normal distribution. In the results of kurtosis in Fig. 14, the kurtosis value of scrambled image is closer to zero than original image. Thus, the difference between any two coefficients in the scrambled image is smaller. In other words, when we randomly construct two trees as the wavelet-tree-based schemes do, the energy of two trees in a pair will be close. If the energy is close, the difference of energy after tree quantization will be more apparent. So, the detection of watermark will be more accurate.

The absolute value of log energy entropy means the magnitude of the information contained in the image. If there is more coefficient energy existing in an image, there will be more capacities for embedding the watermark. If the capacity can increase, the payload to embed the watermark can be also increased to enhance the watermark security. This observation is also reflected in Fig. 15 for all 12 testing images.

From the feature statistic analysis, we can clearly understand the reason why applying the chaotic system can enhance the security robustness. After examining the extensive experimental results with the mathematical feature analysis, the collaboration of chaotic system with wavelet tree based watermarking algorithms proved such design is feasible and very useful in applications.

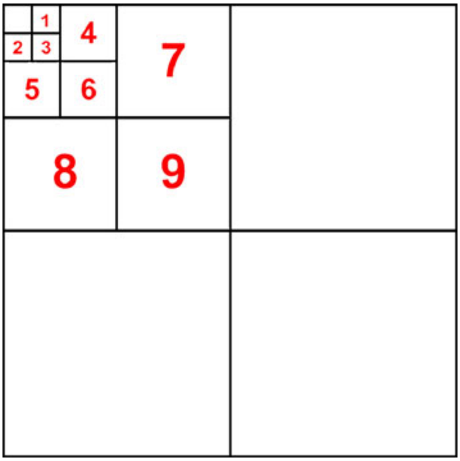


Fig. 11 Wavelet subbands used for feature analysis

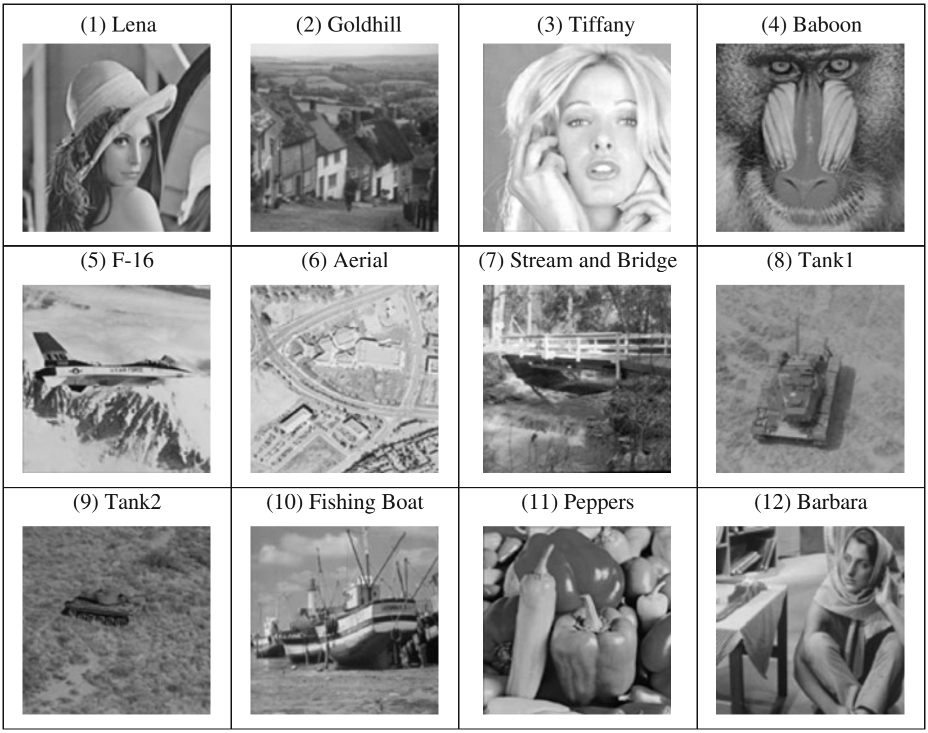


Fig. 12 The testing Images

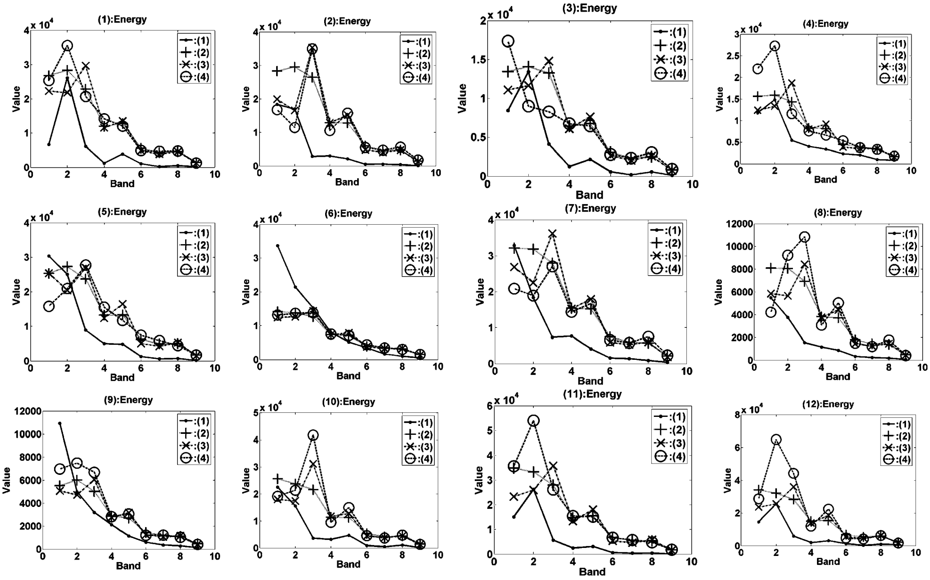


Fig. 13 The statistical results of Energy feature for 12 testing images. Inside each plot, (1) is the original image (2) is the image applied by random ordering (3) is the image scrambled by Fibonacci transformation and (4) is the image applied by Toral Automorphism

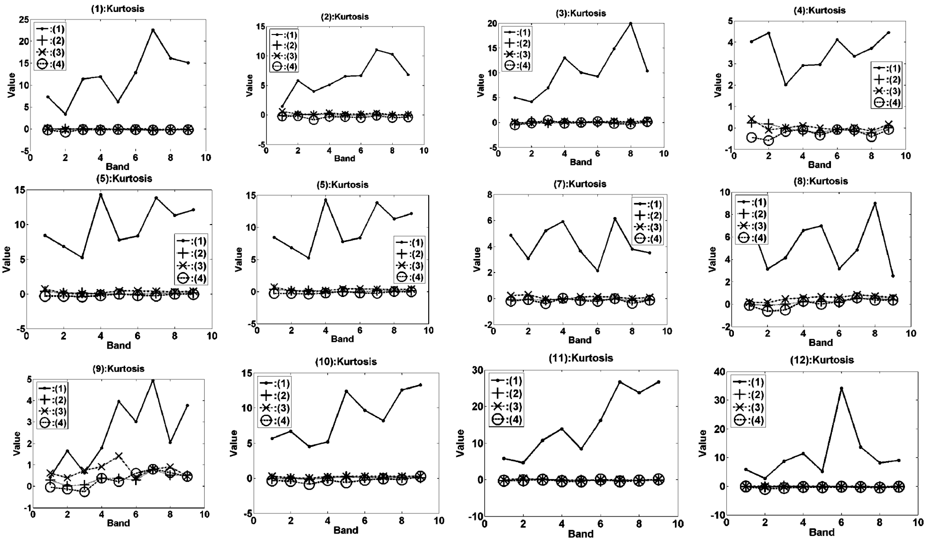


Fig. 14 The statistical results of Kurtosis feature for 12 testing images. Inside each plot, (1) is the original image (2) is the image applied by random ordering (3) is the image scrambled by Fibonacci transformation and (4) is the image applied by Toral Automorphism

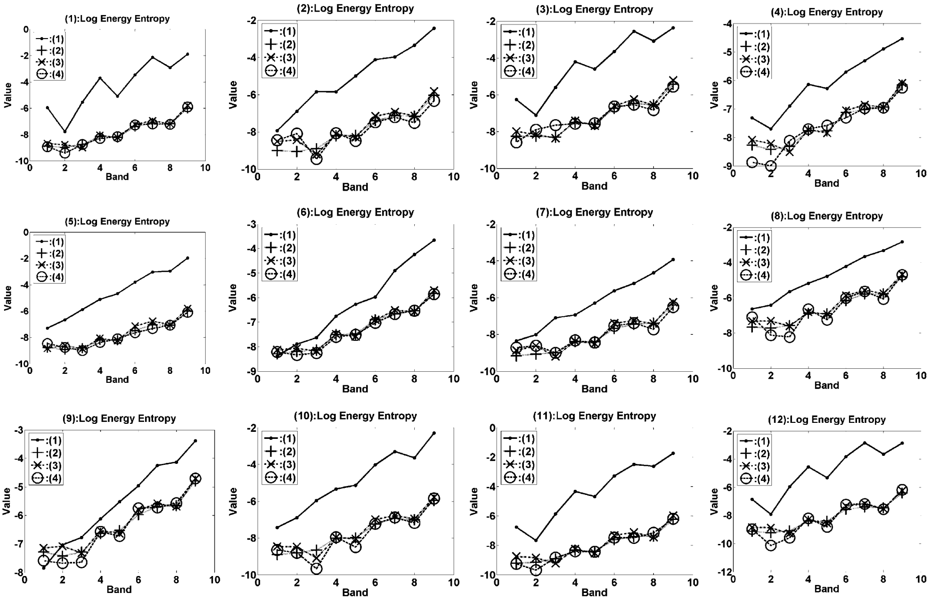


Fig. 15 The statistical results of Log Energy Entropy feature for 12 testing images. Inside each plot, (1) is the original image (2) is the image applied by random ordering (3) is the image scrambled by Fibonacci transformation and (4) is the image applied by Toral Automorphism

5.1 Future research

In general, images from different categories have different inherent characteristics [14, 15]. For example, it is a common observation that most of the natural images are continuous tone compared to the synthetic images most of which are discrete tone that is the dynamic range of the pixel bit depth are under utilized. Such images generally have some numerical structures that are not well represented by smooth basis functions. Even within a particular category, images vary in many ways with widely varying first and second order Markov statistics. Whereas some are relatively flat, others are very busy having more edges and contours in them. So, an analysis of these images shows different characteristics like mean, median, variance and histogram in the spatial domain. In order to get further mathematical expression consideration, different images under various spatial domain characteristics should be investigated. In addition, spectral flatness measure (SFM) [13] to determine the overall image activity will be studied. The transform coefficients of various subbands (including the transform coding gain (TCG) [6, 9] which measures the energy compaction of the transform for different wavelet filters used) should be analyzed. As a result, these factors should help to determine the characteristics of the chaotic system after transformation for better performance and the mathematical expression of the relationship from chaotic system to the transform subband can be theoretically analyzed.

6 Conclusion

How to improve the robustness of wavelet tree based digital image watermarking techniques is discussed in this study. Owing to the weakness of WTQ, Das and Maitra have addressed cryptanalysis attack on WTQ. In order to fix this weakness, this paper has addressed this issue by applying chaotic system to enhance the security of wavelet tree based watermarking algorithms like WTQ, WTGM and DEED. Through our extensive experiments, the simulation results demonstrate that the effectiveness of using chaotic systems for WTQ, WTGM and DEED algorithms improves the security robustness, especially, to resist the cryptanalysis attack.

Acknowledgments The author would like to thank the anonymous reviewers with their valuable comments to improve the quality of this manuscript. This work is partially supported by the National Science Council in Taiwan, Republic of China, under Grant NSC96-2416-H009-015, NSC97-2410-H009-034 and 99-2918-1-009-008.

References

1. Battisti F, Carli M, Neri A, Egiazarian K (September 10–12 2007) Image watermarking in the Fibonacci-Haar transform domain. International Workshop on Nonlinear Signal and Image Proc., Bucharest, Romania, pp 15–19
2. Cox IJ, Linnartz JP (1998) Some general methods for tampering with watermarks. IEEE J Sel Areas Commun 16(4):587–593
3. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1658
4. Das TK, Maitra S (2004) Cryptanalysis of wavelet tree quantization watermarking scheme. IWDC 2004, LNCS 3326, pp 219–230
5. Das TK, Maitra S, Mitra J (2005) Cryptanalysis of optimal differential energy watermarking (DEW) and a modified robust scheme. IEEE Trans Signal Process 53(2):768–775
6. He Z (2007) Peak transform for efficient image representation and coding. IEEE Trans Image Proc 16 (7):1741–1754
7. Kalker T (Oct 3–5 2001) Considerations on watermarking security. Proceedings of the IEEE Workshop on Multimedia Signal Proc, pp 201–106

8. Kerckhoffs A. La Cryptographie Militaire. Journal des Sciences Militaires, 9th series, pp. 5–38, Jan. 1883, pp.161–191, Feb, 1883
9. Kok CW, Nguyen TQ (1998) Multirate filter banks and transform coding gain. IEEE Trans Signal Process 46(7):2041–2044
10. Kundur D, Hatzinakos D (1998) Digital watermarking using multiresolution wavelet decomposition. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing 5:2869–2972
11. Langelaar GC, Lagendijk RL (2001) Optimal differential energy watermarking of DCT encoded images and video. IEEE Trans Image Process 10(1):148–158
12. Lu CS, Huang SK, Sze CJ, Liao HY (2000) Cocktail watermarking for digital image protection. IEEE Trans Multimedia 2(4):209–224
13. Rao S, Pearlman WA (1996) Analysis of linear prediction, coding, and spectral estimation from subbands. IEEE Trans Inf Theory 42(4):1160–1178
14. Saha S, Vemuri R (Nov. 1999) Adaptive wavelet filters in image coders—How important are they? Proc. IEEE/IECON'99, vol. 2, San Jose, CA, pp 559–564
15. Saha S, Vemuri R (2000) An analysis on the effect of image features on lossy coding performance. IEEE Signal Proc Lett 7(5):104–107
16. Said A, Pearlman WA (1996) A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Trans Circuits Syst Video Technol 6:243–250
17. StirMark, [Online]: http://www.petitcolas.net/fabien/software/StirMarkBenchmark_4_0_129.zip.
18. Tsai MJ (accepted for publication in 2009) Dynamic Energy Enabled Differentiation (DEED) Image Watermarking Based on Human Visual System and Wavelet Tree Classification. Multimedia Tools and Applications
19. Tsai MJ, Shen CH (2007) Wavelet Tree Group Modulation (WTGM) for digital image watermarking. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing 2:173–176
20. Tsai MJ, Shen CH (2008) Differential energy based watermarking algorithm using Wavelet Tree Group Modulation (WTGM) and human visual system. IEICE E91-A(8):1961–1973
21. Tsai MJ, Yu KY, Chen YZ (2000) Joint wavelet and spatial transformation for digital watermarking. IEEE Trans Consum Electron 241–245
22. USC SIPI - The USC-SIPI Image Database [Online]. Available: http://sipi.suc.edu/services/database/Database.html.
23. Voyatzis G, Pitas I (Sep 16–19 1996) Applications of toral automorphisms in image watermarking. International Conference on Image Processing 1237–1240, Lausanne, Switzerland
24. Wang SH, Lin YP (2004) Wavelet tree quantization for copyright protection watermarking. IEEE Trans Image Process 13(2):154–165
25. Zou J, Ward RK, Qi D (2004) The generalized Fibonacci transformations and application to image scrambling. Acoust Speech Signal Process 3:385–388

Min-Jen Tsai received the B.S. degree in electrical engineering from National Taiwan University in 1987, the M.S. degree in industrial engineering and operations research from University of California at Berkeley in 1991, the engineer and Ph.D. degrees in Electrical Engineering from University of California at Los Angeles in 1993 and 1996, respectively. From 1996 to 1997, he was a senior researcher at America Online Inc. In 1997, he joined the institute of information management at the National Chiao Tung University in Taiwan and is currently an associate professor. His research interests include multimedia system and applications, image forensic, digital watermarking and authentication, web service, enterprise computing for electronic commerce applications.