NDFT-based Image Steganographic Scheme with Discrimination of Tampers

Hongxia Wang and Mingquan Fan
School of Information Science and Technology, Southwest Jiaotong University
Chengdu, 610031 - P.R.China
[e-mail: hxwang@swjtu.edu.cn, mqfan_sc@163.com]
*Corresponding author: Hongxia Wang

Received August 18, 2011; revised November 6, 2011; accepted November 24, 2011; published December 31, 2011

Abstract

A new and secure image steganographic scheme based on nonuniform discrete Fourier transform (NDFT) is proposed in this paper. First, the chaotic system is introduced to select embedding points randomly in NDFT domain suitable range, and NDFT is implemented on every non-overlapping block of eight consecutive pixels. Second, the secret messages are scrambled by chaotic systems, and embedded into frequency coefficients by quantization method. The stego-image is obtained by inverse NDFT (INDFT). Besides, in order to discriminate tampers, the low frequency wavelet coefficients of 7 most significant bits (MSBs) of the stego-image are converted into the binary sequence after nonuniform scalar quantization. Then the obtained binary sequence is scrambled by the chaotic systems, and embedded into the least significant bit (LSB) of the stego-image. Finally, the watermarked stego-image can be obtained by a new improved LSB steganographic method. The embedded secret messages can be extracted from the watermarked stego-image without the original cover image. Experimental results show the validity of the proposed scheme, and dual statistics attacks are also conducted to indicate the security.

Keywords: Steganography, NDFT, stego-image, fragile watermark, chaos

This research was supported by the National Natural Science Foundation of China (NSFC) under the grant No. 61170226, and the Fundamental Research Funds for the Central Universities under the grant No. SWJTU11CX047.

DOI: 10.3837/tiis.2011.12.005

1. Introduction

Recent years, the wide spread of Internet has created a strong need to protect illegal data. The conventional cryptography offers the ability to transmit information between the users that prevents others from observing it. A new private-key cryptosystem based on the concatenation of codes was proposed to avoid the weakness in some PRAE systems [1]. An image encryption algorithm based on the chaotic Chua's circuit with piecewise linear (PWL) memristor was proposed in [2]. This algorithm meets the principle of Kerchhoff, and the key belongs to the set of real number, so the key space is large, and it can resist brute-force attack. Although these encryption methods have a super security, the attacker often decrypts the cipher-text by the cryptanalysis method or chaos reconstruction [3][4][5][6]. Even if the adversary cannot decrypt the encrypted message, he or she can destroy the cipher-text such that the legal user cannot obtain the plaintext. So the secure communication becomes unsafe. Consequently, the steganography technique, as an important branch of information hiding, has come to many attentions in recent years. In steganography, a message signal is embedded into a host or cover signal to get a composite or stego-signal in such a way that the presence of hidden information cannot be detected by either statistical or perceptual analysis of the stego-signal [7][8]. In this paper, we propose a new image steganographic scheme with discrimination of tampers based on nonuniform discrete Fourier transform (NDFT). Moreover, a new improved LSB (least significant bit) embedding method is used in this scheme, which enhances the security of the proposed steganographic scheme greatly. The remainder of this paper is organized as follows. Section 2 described the related works and 1-D NDFT. The data embedding and extracting process is presented in Section 3. Section 4 gives several experimental results and security analysis. Finally, the conclusions are stated in Section 5.

2. Related Works and 1-D NDFT

2.1 Related Works

Up to now, a lot of research works of steganography have been presented [9][10][11]. The spatial-domain LSB replacement is a popular and simple type of steganography [12]. It combines high capacity with extreme ease of implementation. Moreover, the stego-image is visually imperceptible. Many steganography tools available on the Internet use some form of LSB replacement, but in fact it is highly vulnerable to statistical analysis [13][14][15]. In addition, as we known, transform-domain data hiding schemes have better image quality and larger hiding capability than spatial-domain schemes. Consequently, the transform-domain steganography is researched popularly in these years. One of the typical representations is quantifying DFT (discrete Fourier transform) parameters (amplitude or phase) to embed secret information [16][17]. However, the traditional DFT has a limitation of public and fixed frequency points in frequency domain. That is, for transform-domain attacks, the embedding position is not a secret for intruders although the embedding position is unknown in spatial domain such as spread spectrum. The mere existence of such flaws indicates that the hackers could tamper easily the secret information in frequency domain for DFT-based steganographic schemes because of the public and fixed transform.

Therefore, aiming at the DFT-based data hiding scheme vulnerable to transform-domain attacks, we use NDFT with nonuniformly-spaced samples in frequency domain to design a

new and secure image steganographic scheme in this paper. The secret messages are scrambled by chaotic systems, then embedding the scrambled binary sequence into the NDFT-domain coefficients by quantization method to get the stego-image. Furthermore, the low frequency wavelet coefficients of 7 most significant bits (MSBs) of the stego-image are used as fragile watermark to be embedded into the LSB of the stego-image by our improved LSB steganographic method. In this case, the receiver can detect whether the embedded secret messages to be tampered or not, besides he/she can locate the tampered position. Theoretical analysis and experimental results show our scheme not only has the ability of resisting malicious attack, χ^2 method and RS (regular-singular) statistical analysis, but also can discriminate different tampers.

2.2 1-D NDFT

The NDFT of a sequence $y[n]$ with length N is defined as [18]

$$Y(z_k)=\sum_{n=0}^{N-1} y[n] z_k^{-n}, k=0,1,\cdots,N-1 \tag{1}$$

where, $z_0, z_1, \cdots, z_{N-1}$ are arbitrary N different points located on the z-plane. A matrix form of Eq.(1) is described as follows:

$$Y = Dy \tag{2}$$

Here,

$$Y=\begin{bmatrix} Y(z_0) \\ Y(z_1) \\ \vdots \\ Y(z_{N-1}) \end{bmatrix}, \quad y=\begin{bmatrix} y[0] \\ y[1] \\ \vdots \\ y[N-1] \end{bmatrix}, \quad D=\begin{bmatrix} 1 & z_0^{-1} & z_0^{-2} & \cdots & z_0^{-(N-1)} \\ 1 & z_1^{-1} & z_1^{-2} & \cdots & z_1^{-(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & z_{N-1}^{-1} & z_{N-1}^{-2} & \cdots & z_{N-1}^{-(N-1)} \end{bmatrix}$$

where, D is a Vandermonde matrix and it can be entirely determined by N points z_k, k=0, 1, …, N-1. A factored form of D can be described as:

$$\det(D)=\prod_{i\neq j, i>j}\left(z_i^{-1}-z_j^{-1}\right) \tag{3}$$

So D is nonsingular.Therefore, the inverse NDFT (INDFT) exists and is unique as follows:

$$y = D^{-1}Y \tag{4}$$

In this paper, $\{z_k \mid k=0,1,2,\cdots,7\}=\{0,\pi/4, f, 3\pi/4, \pi, 5\pi/4, 2\pi-f, 7\pi/4\}$. Where, the frequency point f should be chosen from the NDFT-domain suitable frequency range. According to [19], that is $f\in(817\pi/2028, 1329\pi/2028)$, and f is the integral times of $\pi/2048$.

3. Proposed Data Hiding

3.1 Application of Chaos in Data Hiding Process

In our scheme, a binary image is used as secret message. We simply divide the gray-scale cover image into many non-overlapping blocks of eight consecutive pixels, then NDFT is implemented on every block by the chaotic system selecting randomly the embedding points. Subsequently, we use the chaotic system to scramble the secret message. Finally, the

scrambled binary sequence is embedded into NDFT-domain coefficients by quantization method, and the stego-image is obtained by INDFT. The more details are described as follows.

Based upon the sensitive dependence of chaotic systems on their initial conditions, a large number of non-periodic, noise-like, yet deterministic and reproducible signals can be generated. In our proposed scheme, a chaotic sequence generated by the Logistic map is used to choose randomly the special embedding points in NDFT-domain suitable frequency range, which could make the embedding frequency points private. Thus, the transform-domain attack is avoidable.

The Logistic map is defined as follows:

$$x_{n+1} = \lambda x_n (1 - x_n), n = 0,1,2,\cdots \tag{5}$$

Here, $x_n \in (0,1)$, and when $\lambda \in (3.57, 4]$, the Logistic system appears a chaotic state. In our scheme, the initial condition x_0 and the chaotic parameter λ are as keys, denoted as K_1 and K_2, respectively.

In order to resist so-called copy attack, we use chaotic sequence to scramble the secret information before being embedded into NDFT-domain coefficients. The scrambling process is detailed described as follows:

Step1. Segment the binary image W of size $m_1 \times m_2$ into non-overlapping blocks with size of 2×2, noted as $I_{Lb} = \{I_{Lb(i)} \mid i = 1,2,\cdots,(m_1 \times m_2)/(2 \times 2)\}$.

Step2. Generate a chaotic sequence by (5) with K_1 and K_2, denoted as p_n, which is used in the following chaotic map

$$s_{n+1} = (1 + 0.3(s_{n-1} - 1.08) + 379 s_n^2 + 1001 p_n^2) \bmod 3,\ n = 1,2,\cdots,L \tag{6}$$

According to (6), a multiple value chaotic sequence noted as S is produced. In Eq. (6), two chaotic initial values s_0 and s_1 are considered as systematic secret keys. When s_0, $s_1 \in$ (-1.5, 1.5), the chaotic map possesses chaotic attractor [20]. From the view point of chaotic characteristics, the chaotic sequence has a longer period due to adding the parameter p_n, which makes the chaotic system very unpredictable, sensitive to the initial chaotic values, and have an ability to resist the finite word length effect. For the whole chaotic system, s_0 and s_1 are noted as K_3 and K_4, respectively. Therefore, the secret keys of whole scrambling encryption could be concluded as K={ K_1, K_2, K_3, K_4}.

Step3. To obtain the address sequence A for scrambling I_{Lb}, the elements of chaotic sequence S is sorted in ascending order, such that $S_{a_1} \le S_{a_2} \le \ldots \le S_{a_L}$. The position of each element $S_{a_1}, S_{a_2}, \ldots, S_{a_L}$ in chaotic sequence S is formed the address sequence A, noted as A={a_1, …, a_i, …, a_L| a_i=1,2,…, L}.

Step4. Scramble I_{Lb} by using the ordered address sequence A. The sketch map is shown in **Fig. 1**. The binary matrix I_{Lb} is divided into the same size blocks. nk and mk are as the number of blocks for every row and column, respectively. In **Fig. 1**, L=mk×nk, and

$$\begin{cases} i_w = \lfloor (A(temp_{ij}) - 1)/nk \rfloor + 1 \\ j_w = A(temp_{ij}) - (i_w - 1)nk \\ temp_{ij} = (i_{Lb} - 1)nk + j_{Lb} \end{cases}$$

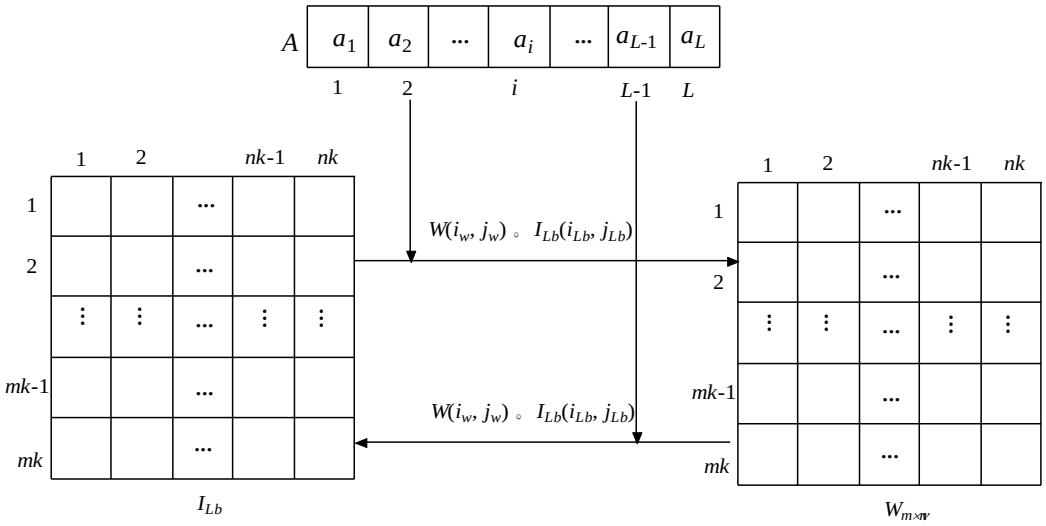


Fig. 1. Sketch map of scrambling and retrieving the binary image

3.2 Secret Message Embedding

The details of embedding secret message are described as follows:

Step1. Segment the gray-scale cover image into many non-overlapping blocks of eight consecutive pixels, each block is noted as $I(k)$;

Step2. Generate chaotic sequence X with K_1 and K_2 by Eq. (5), then multiply X with 514 to select an embedding frequency points f for each block $I(k)$ in the NDFT-domain suitable frequency range;

Step3. Carry out NDFT with the chosen frequency points for every block

$$Fe(k) = NDFT(I(k), f) \tag{7}$$

Step4. As shown in **Fig. 2**, select a frequency coefficient corresponding to f in $Fe(k)$, noted as $Fe_1(k)$. Quantize the amplitude of $Fe_1(k)$ to embed 1-bit secret message which is processed from I_{Lb} by above scrambling process.

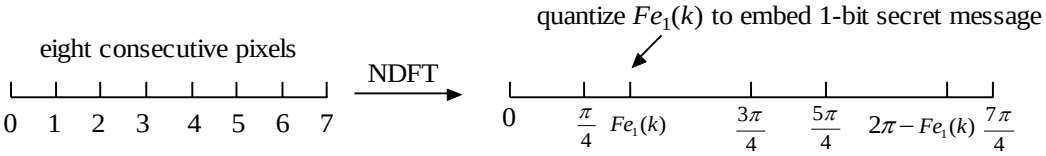


Fig. 2. Sketch map of embedding secret message

The basic idea of quantization method is described as follows. $\left|Fe_1^Q(k)\right|$ is adjusted to the center of the nearest quantization interval away from $|Fe_1(k)|$. That is to say, the axis is divided into A and B sets according to quantization step Δ, when $W(k)=1$, $\left|Fe_1^Q(k)\right|$ is adjusted to the center of A set; when $W(k)=0$, $\left|Fe_1^Q(k)\right|$ is adjusted to the center of B set.

Calculate $m = \lfloor |Fe_1(k)| / \Delta \rfloor$, and $r = |Fe_1(k)| - m \times \Delta$, where $\triangle$ is quantization step. The quantization rule is depicted as follows:

When $m = 0$, the quantized coefficient $\left|Fe_1^Q(k)\right|$ is

$$\left|Fe_1^Q(k)\right| = \begin{cases} \Delta/2, & W(k)=1 \\ 3\Delta/2, & W(k)=0 \end{cases} \tag{8}$$

When $m \neq 0$, the quantized coefficient $\left|Fe_1^Q(k)\right|$ is

$$\left|Fe_1^Q(k)\right| = \begin{cases} \begin{cases} 2k\Delta+\Delta/2, & if\ m=2k \\ 2k\Delta+\Delta/2, & if\ m=2k+1 \quad and \quad |r|\le\Delta/2 \\ 2k\Delta+2\Delta+\Delta/2, & if\ m=2k+1 \quad and \quad |r|>\Delta/2 \end{cases}, & W(k)=1 \\ \begin{cases} (2k+1)\Delta+\Delta/2, & if\ m=2k+1 \\ 2k\Delta-\Delta/2, & if\ m=2k \quad and \quad |r|\le\Delta/2 \\ (2k+1)\Delta+\Delta/2, & if\ m=2k \quad and \quad |r|>\Delta/2 \end{cases}, & W(k)=0 \end{cases} \tag{9}$$

To guarantee the embedded values still be real number by INDFT, the data embedding process is implemented under the positive symmetric condition. That is, for the chosen frequency point, let $f(k) = f^*(N-k)$. The positive symmetric condition is defined as

$$\left|F(k)\right| \leftarrow \left|F(k)\right| + \varepsilon \tag{10a}$$

$$\left|F(N-k)\right| \leftarrow \left|F(N-k)\right| + \varepsilon \tag{10b}$$

Step5. Perform inverse NDFT on the embedded frequency coefficient, the stego-image blocks is obtained by

$$I_s(k) = INDFT(Fe_1^Q(k), f) \tag{11}$$

Step6. Joint all of image blocks as the stego-image I_S.

3.3 Fragile Watermark Embedding

Generally speaking, if the stego-image is destroyed, the secret message will not be extracted exactly by the receiver. In order to detect whether the stego-image is destroyed or not, and seek the tampered position under the condition of being destroyed, the idea of fragile watermark is introduced. The fragile watermark embedding process is depicted in **Fig. 3**, and the details are illustrated as follows:

Step1. Set the LSB of the stego-image I_S to zero, and obtain $\tilde{I}_s$. Then, we perform 2D wavelet decomposition on $\tilde{I}_s$, and note the low frequency coefficients as *CA*.

Step2. Utilize nonuniform scalar quantization method to quantize each coefficient of *CA* to 4-bit size, so a low frequency compressed image I_L is obtained. The details of quantization rule are shown as follows:

$$I_L = \begin{cases} k, & CA \in [CA_{\min} + kq + \sigma_k, CA_{\min} + (k+1)q + \sigma_{k+1}) \\ 15, & CA = CA_{\max} \end{cases} \tag{12}$$

where, $CA_{\min}$ and $CA_{\max}$ means the maximal and minimal coefficients of *CA*, respectively; $q = \lceil (CA_{\max} - CA_{\min})/32 \rceil$, and $\sigma_k \in (-q/4, q/4)$, $k = 0,1,2,\cdots,15$.

Step3. Covert each pixel of the low frequency compressed image I_L into 4-bit binary sequence $(b_3 b_2 b_1 b_0)_2$, then a binary matrix is obtained by

$$(b_3b_2b_1b_0)_2 \rightarrow [I_{Lb}]_{2\times 2} = \begin{bmatrix} b_3 & b_2 \\ b_1 & b_0 \end{bmatrix} \tag{13}$$

Step4. Scramble the binary matrix I_{Lb} by the scrambling method described in subsection 3.1 to obtain the fragile watermark W_{Lb}.

Step5. Every element of W_{Lb} is embedded into the LSB of I_s by our improved LSB steganographic method, and the watermarked stego-image I_s^w is obtained. The improved LSB steganographic method is depicted as follows:

Set two variables N_{up} and N_{down} that represent the plus 1 and minus 1 times of pixels when the fragile watermark is embedded, respectively. If the watermark bit is same as the LSB of the corresponding pixel, the pixel value will not change. Else, we embed a watermark bit according to the following rule

$$I_s^w(i,j) = \begin{cases} I_s(i,j)+1, & if\ I_s(i,j)=0 \quad or \quad N_{up} < N_{down} \\ I_s(i,j)-1, & if\ I_s(i,j)=255 \quad or \quad N_{up} \geq N_{down} \end{cases} \tag{14}$$

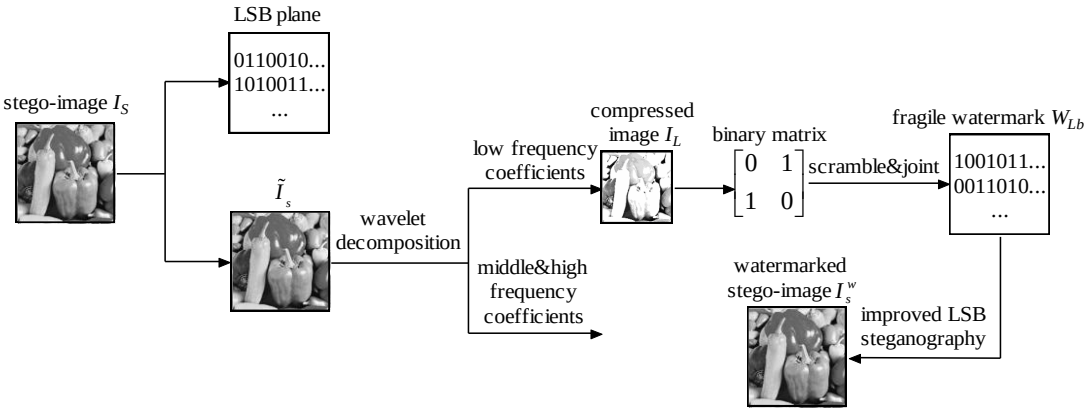


Fig.3. Fragile watermark embedding process

3.4 Extraction of Hidden Information and Low Frequency Compressed Image

In our scheme, the extraction process of hidden information and the low frequency compressed image need not the original image. The extraction process is inverse to the embedding process. The extraction process of hidden information is discribed as follows:

Step1. Set LSB of the watermarked stego-image I_s^w to zero to get $\tilde{I}_1$, then segment $\tilde{I}_1$ into many non-overlapping blocks of eight consecutive pixels, and note each block as $\tilde{I}_1(k)$.

Step2. Carry out NDFT for each $\tilde{I}_1(k)$ with the same embedding frequency points and chaotic keys as follows

$$Fe'(k) = NDFT(\tilde{I}_1(k), f) \tag{15}$$

Step3. As shown in **Fig.4**, select a frequency coefficient corresponding to f in $Fe'(k)$, noted as $Fe_1'(k)$, the hidden information bit is extract by

$$W'(k)=\begin{cases}1, & |Fe_1'(k)|\in A\\ 0, & |Fe_1'(k)|\in B\end{cases} \tag{16}$$

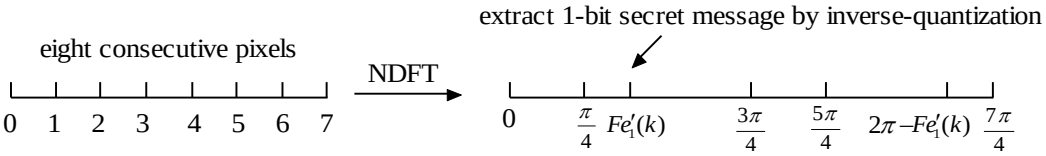


Fig. 4. Sketch map of extracting secret message

The steps of extracting the low frequency compressed image are given as follows:

Step1. Distill the LSB of the watermarked stego-image I_s^w, and covert these bits into a binary matrix I'_{Lb}, which is the fragile watermark.

Step2. Inversely scramble the binary matrix I'_{Lb} by the method described in subsection 3.1 to obtain a new matrix I''_{Lb}.

Step3. According to Eq. (17), I'_L is obtained by I''_{Lb}. Every I'_L combines into the low frequency compressed image.

$$[I''_{Lb}]_{4\times4}=\begin{bmatrix}b'_3 & b'_2\\ b'_1 & b'_0\end{bmatrix}\rightarrow(I'_L)=(b'_3b'_2b'_1b'_0)_2 \tag{17}$$

4. Experimental Results and Analysis

4.1 Experimental Results

In our experiments, four 256×256 standard images "Peppers", "Lena", "Baboon" and "Airplane" are as cover images shown in **Fig. 5**. The binary image "swjtu.bmp" of size 64×64 is as the secret message. Let K_1=0.5, K_2=4, K_3=1, K_4=0.8, △=2000, the peak signal-to-noise ratios (PSNRs) [21] for the watermarked stego-image "Peppers", "Lena", "Baboon" and "Airplane" are 41.5 dB, 39.8 dB, 42.9 dB and 38.7 dB, respectively. The binary secret image and its scrambled result by the Logistic chaotic system are shown in **Fig. 6**. Obviously, the scrambled image is very random.

(a) Peppers **(b)** Lena **(c)** Baboon **(d)** Airplane

Fig. 5. Cover images

As an example, **Fig. 7** shows the stego-image "Peppers" carrying secret message, the

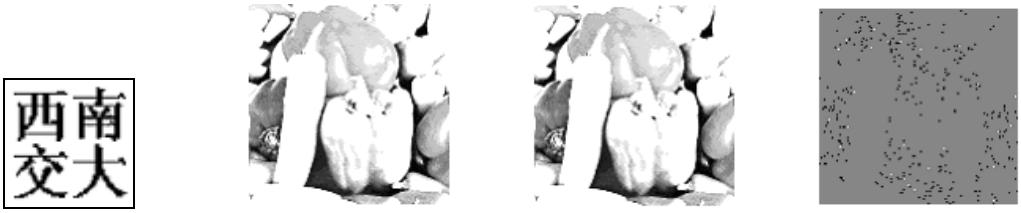
compressed low frequency image generated from 7 MSBs of stego-image, and the final watermarked stego-image after embedding the low frequency compressed image by the improved LSB steganographic scheme. Obviously, both the stego-image and watermarked stego-image show a good visual imperceptibility. **Fig. 8-(a)** shows the extracted hiding message from LSB of the watermarked stego-image. **Fig. 8-(b)** shows the extracted compressed image from LSB of the watermarked stego-image. **Fig. 8-(c)** shows the generated compressed image from 7 MSBs of the watermarked stego-image, and **Fig. 8-(d)** shows the difference between two compressed images. From **Fig. 8**, it can be seen that our scheme can extract correctly hiding information without the original image and two compressed images.

(a) Secret image **(b)** Scrambled image

Fig. 6. Binary secret image and scrambled image

(a) Stego-image **(b)** Compressed low frequency image **(c)** Watermarked stego-image

Fig. 7. Scrambled secret message and fragile watermark are embed into “Peppers” image



(a) Extracted hiding message **(b)** Extracted compressed image **(c)** Generated compressed image **(d)** Difference between two compressed images

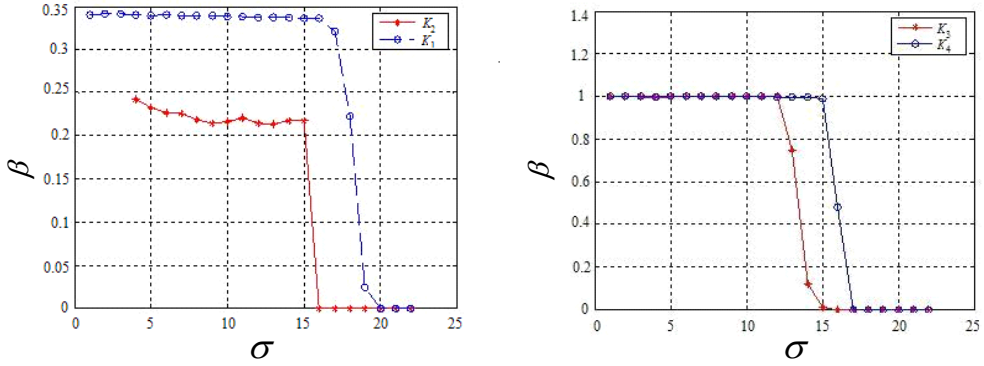
Fig. 8. Extracted hiding message, two resumptive low frequency compressed images, and difference between two compressed images

4.2 Security of Resisting Malicious Attack

In this paper, we use chaotic sequence to select the private embedding position, scramble the hidden important messages and the low frequency compressed image. The initial condition x_0 and the chaotic parameter λ of the Logistic map and the initial condition s_0, s_1 of Eq. (6) are used as keys K_1, K_2, K_3, K_4, respectively. Because these keys possess real-valued numbers, so a

large number of non-periodic noise-like chaotic sequences can be generated.

In the proposed scheme, the NDFT-domain suitable frequency range brings the probability to hide embedding position, and the embedding points chosen by chaotic sequence enhance the secrecy capability. So the adversary without keys can only attack stego-image with random frequency points by guessing keys. In the process of scrambling the hidden important messages and the low frequency compressed image, K_1, K_2, K_3, K_4 are all used. **Fig. 9** shows the key spaces of K_1-K_2 and K_3-K_4, respectively. Let $10^{-\sigma}$ represent a micro-change of chaotic key values, then the key space is $1/10^{-\sigma}=10^{\sigma}$. Here, $\sigma \in Z^+$ is a negative logarithm of changing the chaotic key. As an example, the chaotic sequence x_n is generated by K_1, and another chaotic sequence x'_n is generated by (K_1+$10^{-\sigma}$). The function $\beta = \sum_{n=0}^{N-1} |x_n - x'_n| / N$ represents a average distance of two chaotic sequences with a tiny change of K_1, which is used to test the key space K_1. The curves of β with K_1-K_2 and K_3-K_4 are shown in **Fig. 9-(a)** and **Fig. 9-(b)**, respectively. We can easily see that when the tiny changes of K_1 , K_2, K_3, and K_4 are equal to 10^{-19}, 10^{-15}, 10^{-14}, 10^{-15}, respectively, β values are near to zero gradually, that means there are part of chaotic initial parameters could result in the same chaotic sequence. So we know that the key spaces of K_1, K_2 are 10^{19} and 10^{15}, respectively, and the whole key space is 10^{34}. It is large enough to insure the security of the embedding points in the NDFT-domain suitable frequency range. Similarly, the key spaces of K_3, K_4 are 10^{14} and 10^{15}, respectively. So the whole key space of scrambling the hided important messages and the low frequency compressed image is 10^{63}. It is large enough to enhance the security of the hidden important message and the low frequency compressed image.



(a) K_1-K_2 **(b)** K_3-K_4

Fig. 9. Key spaces of K_1, K_2, K_3 and K_4

4.3 Capability of Discriminating Tampers

In order to test the capability of discriminating of tampers, we do different attacks to the watermarked stego-image. The attacked images and the hiding message extracted from every tampered image are shown in **Fig. 10** and **Fig. 11**, respectively. There are three kinds of tamper modes in **Fig. 10** as follows: (a) A pepper is added in the stego-image; (b) The LSB of the corresponding modification position in **(a)** is only altered while the 7 MSBs have no change; (C) A pepper is added in the watermarked stego-image. We can know the destroyed secret bits from **Fig.11**. **Fig. 12** and **Fig. 13** show the corresponding low frequency compressed images from the LSB and 7MSBs of attacked images shown in **Fig. 10**. **Fig. 14**

shows the difference of corresponding images between **Fig. 12** and **Fig. 13**. From **Fig. 14**, it is known easily that when only 7 MSBs of the stego-image are tempered, the corresponding difference image presents the block shape. If only LSB of the stego-image is tempered, the corresponding difference image presents the random point shape. While all the bits of altered position in the stego-image are changed, the corresponding difference image presents the block and random point shape. If the MSBs of some pixels are tempered, the altered position can be detected correctly, so the receiver can authenticate whether the received image is unfeigned or not.

(a) Add a pepper in stego-image **(b)** Only alter LSB **(c)** Add a pepper in watermarked stego-image

Fig. 10. Attacked images

(a) Fom **Fig.10(a)** **(b)** From **Fig. 10(b)** **(c)** From **Fig. 10(c)**

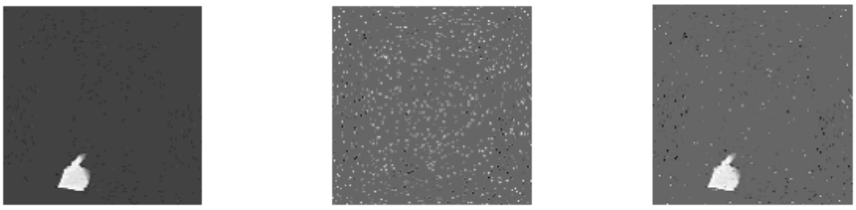
Fig. 11. Hiding message extracted from tampered images

(a) Obtained by **Fig. 10(a)** **(b)** Obtained by **Fig. 10(b)** **(c)** Obtained by **Fig. 10(c)**

Fig. 12. Corresponding resumptive low frequency compressed images from the LSB

(a) Obtained by **Fig. 10(a)** **(b)** Obtained by **Fig. 10(b)** **(c)** Obtained by **Fig. 10(c)**

Fig. 13. Corresponding low frequency compressed images from the 7 MSBs



(a) Fig. 12(a) & **Fig. 13(a)** **(b) Fig.12(b)** & **Fig.13(b)** **(c) Fig.12(c)** & **Fig.13(c)**

Fig. 14. Difference of corresponding images between **Fig. 12** and **Fig. 13**

4.4 Ability of Resisting χ^2 Method and RS Statistical Analysis

(1) Ability to resist χ^2 method

Let h_j represent the appearance times of pixel j in the watermarked stego-image. Suppose the secret bits are uniform distribution bit stream, and the steganographic degree is α, then the following Eq. (18) and Eq. (19) can be obtained

$$h_{2i} = g_{2i} - \frac{\alpha}{2} g_{2i} + \frac{\alpha}{4} g_{2i-1} + \frac{\alpha}{4} g_{2i+1} \tag{18}$$

$$h_{2i+1} = g_{2i+1} - \frac{\alpha}{2} g_{2i+1} + \frac{\alpha}{4} g_{2i} + \frac{\alpha}{4} g_{2i+2} \tag{19}$$

where, g_{2i} means the appearance times of pixel $2i$ in the original image. From Eq. (18) and (19), Eq. (20) can be calculated

$$E(h_{2i+1} - h_{2i}) = (1 - \frac{\alpha}{2})(g_{2i+1} - g_{2i}) + \frac{\alpha}{4}(g_{2i} + g_{2i+2} - g_{2i-1} - g_{2i+1}) \tag{20}$$

where, $E(\cdot)$ means the expectation.From Eq. (20) we know $h_{2i+1} \neq h_{2i}$ even if $\alpha = 1$. So our improved LSB steganographic method can resist χ^2 method successfully.

(2) RS statistical analysis

Let F_1 and F_{-1} represent the transforms between $2i$ and $2i+1$, $2i-1$ and $2i$, respectively. When we embed the fragile watermark into LSB of the stego-image by our improved LSB steganographic method, there are about half secret bits are same as the LSB of pixels, so half of corresponding pixels need not change. However, another half pixels need change. In these pixels which need change, half of them changes from $2i$ to $2i+1$ or from $2i+1$ to $2i$, that is equal to F_1; half of them changes from $2i$ to $2i-1$ or from $2i+1$ to $2i+2$, that is equal to F_{-1}. So when RS statistical analysis is used to analyze the watermarked stego-image, the same confusion of the stego-image appears, and the analytic results will be $R_M \approx R_{-M}$ and $S_M \approx S_{-M}$ in spite of F_1 or F_{-1} transform. **Fig. 15** shows the RS-diagrams yielded by the dual statistics method for the watermarked stego-image. It is shown that our method can resist RS statistical analysis.

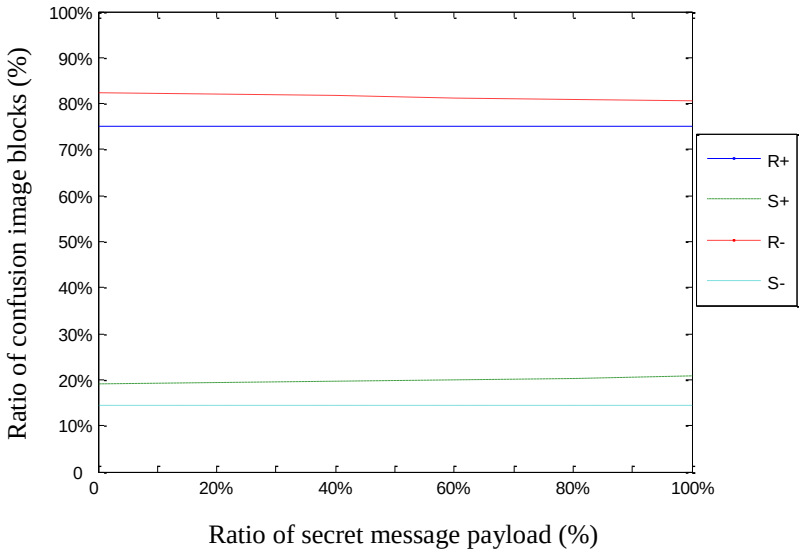


Fig. 15. RS-diagrams yielded by the dual statistics method for the watermarked stego-image

5. Conclusion

In this paper, a new and secure steganographic scheme for embedding important secret messages into a gray-scale cover image is proposed based on NDFT and fragile watermark technique. The scheme utilizes the chaotic system to select randomly the embedded points to implement NDFT on every non-overlapping block of eight consecutive pixels, and quantizes NDFT frequency coefficients to hide secret messages. Analysis shows a large key space ensures the security of the steganographic system. Besides, after nonuniform scalar quantization and being scrambled by the couple chaotic systems, the low frequency wavelet coefficients of 7 MSBs of the stego-image are converted into binary sequence as fragile watermark to be embedded into the stego-image by an improved LSB steganographic scheme. The final watermarked stego-image is obtained. So the receiver can contrast the low frequency compressed image from the LSB of the watermarked stego-image with that of the 7 MSBs to detect whether the image is tempered or not, which enhances the security of the steganographic system greatly. At the same time, the improved LSB steganographic scheme ensures our scheme can resist χ^2 method and RS statistical analysis.

References

[1] A. K. Al Jabri, F. Al-Thukair and A. Mirza, "Private-key Encryption based on Concatenation of Codes," *IEE Proceedings Communications*, vol. 141, no. 3, pp. 105-110, Mar. 1994. Article (CrossRef Link)

[2] Z. H. Lin and H. X. Wang, "Efficient Image Encryption using Chaos-based PWL Memristor," *IETE Technical Review*, vol. 27, no. 4, pp. 318-325, June 2010. Article (CrossRef Link)

[3] X. Li, J. W. Niu, J. Ma,W. D. Wang and C. L. Liu, "Cryptanalysis and Improvement of a Biometrics-based Remote User Authentication Scheme using Smart Cards," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 73-79, Jan. 2011. Article (CrossRef Link)

[4] J. Sung, "Differential Cryptanalysis of Eight-round SEED," *Information Processing Letters*, vol. 111, no. 10, pp. 474-478, Apr. 2011. Article (CrossRef Link)

[5] M. H. Lim, B. M. Goi and S. G. Lee, "An Analysis of Group Key Agreement Schemes based on the Bellare-roGaway Model in Multi-party Setting," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 4, pp. 822-839, Apr. 2011. Article (CrossRef Link)
[6] C. D. Toledo-Suárez, "Meta-chaos: Reconstructing Chaotic Attractors from the Separation of Nearby Initial Conditions on Hyperhelices," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2249-2253, Sep. 2010. Article (CrossRef Link)
[7] J. Fridrich, J. Kodovský, V. Holub and M. Goljan, "Steganalysis of Content-adaptive Steganography in Spatial Domain," in *Proc. of 11th Information Hiding*, LNCS, vol. 6958, pp. 102-117, May 2011. Article (CrossRef Link)
[8] Y. F. Huang, S. Y. Tang and J. Yuan, "Steganography in Inactive Frames of VoIP Streams Encoded by Source CODEC," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 296-306, May 2011. Article (CrossRef Link)
[9] C. N. Yang, G. C. Ye and C. Kim, "Data Hiding in Halftone Images by XOR Block-wise Operation with Difference Minimization," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 2, pp. 457-476, Feb. 2011. Article (CrossRef Link)
[10] T. Filler and J. Fridrich, "Fisher Information Determines Capacity of ε-secure Steganography," in *Proc. of 11th Information Hiding*, LNCS, vol. 5806, pp. 31-47, Mar. 2009. Article (CrossRef Link)
[11] H. Zhao and H. X. Wang, "Statistical Analysis of Several Reversible Data Hiding Algorithms," *Multimedia Tools and Applications*, vol. 52, no. 2-3, pp. 277-290, Feb. 2011. Article (CrossRef Link)
[12] W. R. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding," *IBM System Journal*, vol. 35, no. 3-4, pp. 313-336, Apr. 1996. Article (CrossRef Link)
[13] X. P. Zhang, S. Z. Wang and Z. Y. Zhou, "Multibit Assignment Steganography in Palette Images," *IEEE Signal Processing Letters*, vol. 15, no. 10, pp. 553-556, Oct. 2008. Article (CrossRef Link)
[14] X. P. Zhang and S. Z. Wang, "Vulnerability of Pixel-value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security," *Pattern Recognition Letter*, vol. 25, no. 3, pp. 331-339, Mar. 2004. Article (CrossRef Link)
[15] W. Andreas and P. Andreas, "Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools-and Some Lessons Learned," in *Proc. of 3rd Information Hiding*, LNCS, vol. 1768, pp. 61-76, Feb. 2000. Article (CrossRef Link)
[16] A. S. Khashandarag and N. Ebrahimian, "A New Method for Color Image Steganography Using SPIHT and DFT, Sending with JPEG Format," in *Proc. of IEEE International Conference on Computer Technology and Development*, vol. 1, pp. 581-586, Nov. 2009. Article (CrossRef Link)
[17] N. Ghoshal and J. K. Mandal, "A Steganographic Scheme for Colour Image Authentication (SSCIA)," in *Proc. of IEEE International Conference on Recent Trends in Information Technology*, pp. 826-831, June 2011. Article (CrossRef Link)
[18] S. Bagchi and S. K. Mitra, "The Nonuniform Discrete Fourier Transform and its Applications in Application in Filter Design. I. 1-D," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 43, no. 6, pp. 422-433, June 1996. Article (CrossRef Link)
[19] L. Xie, J. S. Zhang and H. J. He, "NDFT-based Audio Watermarking Scheme with High Security," in *Proc. of IEEE 18th International Conference on Pattern Recognition*, vol. 4, pp. 270-273, September 18-20, 2006. Article (CrossRef Link)
[20] J. S. Zhang and L. Tian, "A New Chaotic Digital Watermarking Method based on Private Key," *Journal of China Institute of Communications* (in Chinese), vol. 25, no. 8, pp. 126-131, Aug. 2004. Article (CrossRef Link)
[21] J. C. Yen, "Watermark Embedded in Permuted Domain," *IEE Electronics Letters*, vol. 37, no. 2, pp. 80-81, Jan. 2001. Article (CrossRef Link)

Hongxia Wang received the B.S. degree from Hebei Normal University, Shijiazhuang, in 1996, and the M.S. and Ph.D. degrees from University of Electronic Science and Technology of China, Chengdu, in 1999 and 2002, respectively. She engaged in postdoctoral research work in Shanghai Jiaotong University from 2002 to 2004. Currently she is a professor with School of Information Science and Technology, Southwest Jiaotong University, Chengdu. Her research interests include multimedia information security, intelligent information processing, and the coding technique. She has published 40 peer research papers and wined 6 authorized patents.

Mingquan Fan received the B.S. and Ph.D. degrees from Southwest Jiaotong University, Chengdu, in 2004 and 2010, respectively. Her research interests include information hiding, network security, and the crptography technique. She has published more than 10 research papers.