NOVEL BLIND NON-ADDITIVE ROBUST WATERMARKING USING 1-D CHAOTIC MAP

Dong-jian WANG, Ling-ge JIANG, Guo-rui Feng

Dept. of Electronic Eng., Shanghai Jiaotong Univ., Shanghai 200030, China

ABSTRACT

We propose a novel blind non-additive robust watermarking scheme in this paper. The energy of the watermark is spread to all regions of the host data instead of some individual elements, which entitles the watermark with *imperceptibility* and high *robustness*. A class of 1-D Markov chaotic maps employed to perform host data elements classification and watermark encryption ensures the *security* of the system. To prove the validity of this proposed scheme, some analyses and brief objective comparisons with the popular spread spectrum (SS) scheme are also presented. Simulation results show that our scheme can survive severe processing such as high-ratio JPEG compression, Gaussian noise pollution and histogram equalization.

1. INTRODUCTION

The design of reliable techniques for copyright protection and content verification of multimedia data become an urgent necessity recently. This demand has been addressed by the emergence of a variety of watermarking schemes. Most of the proposed schemes target towards embedding some imperceptible and undetectable information in the original data, which can denotes the copyright or ownership of the data. Usually, *imperceptibility*, *robustness* to attacks and *security* are three main requirements for an acceptable robust watermarking scheme, as discussed in [1,4,6].

We present an original watermarking scheme in this paper. First, multi-bits watermark is embedded non-additively by re-arranging the differential value of the elements subsets with better performance than SS scheme as in [4]. Objective comparisons and rich simulation results support our analyses in the next sections.

2. 1-D MARKOV CHAOTIC MAPS AND WATERMARK ENCRYPTION

2.1.1-D Markov Chaotic Maps

The one-dimensional Markov chaotic map is a discrete dynamic iteration system, which can be formulated as,

$$z_n = f(\alpha, z_{n-1}) = f^n(\alpha, z_0), \quad z_n \in \Omega, n = 1,2,\Lambda \qquad (1)$$

Where, z_0 is the initial state. Parameter α and non-linear function $f(\cdot)$ will decide the behavior of the systems. Values of sequences z_n are constrained in a specific range denoted as Ω. As discussed in [2], the maps can be chaotic if the parameter α is selected properly. For example, the ICMIC map presented by HE and etc. in [2] which is formulated as,

$$z_{n+1} = f(a, z_n) = \sin\left(\frac{\alpha}{z_n}\right), |z_n| \le 1, n = 0,1,2,\Lambda \qquad (2)$$

is chaotic when parameter α is set to proper region, such as $[3,4)$ and etc. All the discussions in this paper only refer to the chaotic case. Usually, *repeatability, sensitivity to initial states* and *inner randomicity* are the most crucial character that can be used in our applications.

Actually, we employ the chaotic maps to produce chaotic sequences that can be used in mark encryption and the watermark embedding/extracting procedures.

2.2.Fast symmetric watermark encryption

Though lack of maturity, encryption based on chaos theory is now under fast developing. In watermarking, we employ the chaotic sequences to encrypt the watermark data with high speed before watermark embedding and entitle the encrypted data with some special characters, e.g., random like and with equal probability to be 0/1.

A sequence of L length is produced using a 1-D chaotic map, e.g. ICMIC map, where L is the length of the watermark data. Then, the sequence is quantified to a binary sequence e with equal probably to be 0 and 1. The sequence e is used to encrypt the binary watermark w by performing $w_{en}(k) = w(k) \oplus e(k), k = 0,1,\Lambda\ ,L-1$. The encrypted watermark w_{en} is equal of being 0 and 1. The decryption procedure is as simple as the encryption one, which can be formulated as $w(k) = w_{en}(k) \oplus e(k)$, $k = 0,1,\Lambda\ ,L-1$. The initial value of the chaotic map to produce encrypting sequence can be protected as secret keys. Only the one with the right key can decrypt the mark and even a one bit false of the key will fail the decryption. Some of the references can be made in Fig. 1,

where the binary image "JTUMCI" is employed as watermark data.

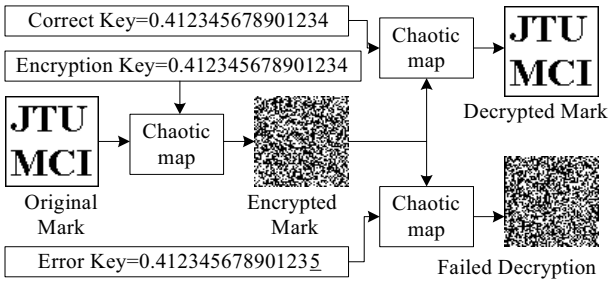


Fig. 1 Symmetric chaotic watermark encryption example

3. WATERMARK EMBEDDING & EXTRACTION

3.1.Watermark embedding algorithm

The watermark-embedding diagram is shown in Fig. 2. The box "Transform" is used to transform the original signal to a domain where the watermark is embedded. In practice, designing or selection of a "good transform" will affect the performance of a specific watermarking algorithm greatly. However, we don't address this problem but try to present a new marking method instead.

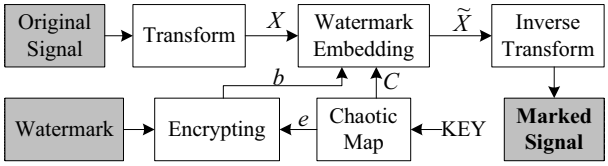


Fig. 2 Watermark embedding diagram

To describe the algorithm, we employ X to denote coefficients to carry a specific encrypted watermark bit $b = 2 \cdot w_{en}(k) - 1, b = \pm 1$. Binary (-1/1) sequence C produced by chaotic maps is used to classify the coordinates of X into two sets, denoted as Ψ_1 and Ψ_2.

$$\begin{cases} i \in \Psi_1 & if \;\; C(i) = -1 \\ i \in \Psi_2 & if \;\; C(i) = 1 \end{cases}, i = 0, \Lambda \; N-1 \tag{3}$$

Here, the numbers of elements in Ψ_1 and Ψ_2 are N_1 and N_2 respectively. Then equations $N_1 + N_2 = N$ and $\Psi_1 \cap \Psi_2 = \Phi$ are satisfied, i.e. Ψ_1 is the complement of set Ψ_2. We calculate difference ξ between the average of the elements of X in Ψ_1 and Ψ_2 as,

$$\xi = \frac{1}{N_1} \sum_{i \in \Psi_1} X(i) - \frac{1}{N_2} \sum_{i \in \Psi_2} X(i) \tag{4}$$

Positive number Δ is employed to control the watermark strength embedded and another variable α is defined as,

$$\alpha = \begin{cases} b \cdot \Delta - \xi, & b \cdot \xi < \Delta \\ 0, & b \cdot \xi \geq \Delta \end{cases} \tag{5}$$

Here, b is the bipolar watermark bit that valued ± 1. Then we embed the watermark bit b by re-arranging the value of each $X(i)$. The resulted signal $\tilde{X}$ will be decided by,

$$\tilde{X}(i) = \begin{cases} X(i) + a/2, & i \in \Psi_1 \\ X(i) - a/2, & i \in \Psi_2 \end{cases} \tag{6}$$

After inverse transformation performed on $\tilde{X}$, the marked signal is reached. Energy of the watermark embedded is decided by selection of Δ , which is reflected by peak signal-to-noise ratio (PSNR) of the marked signal. In fact, it is controlled and distributed to all over the range of the host signal in this algorithm, which ensures the *imperceptibility* of the watermark.

3.2. Watermark extraction algorithm

Watermark extraction is the inverse process of the embedding procedures as in Fig. 3. The test signal is transformed for watermark extraction. The 1-D Markov chaotic map is employed again to reproduce the binary sequences C and e that are used to perform the watermark extraction and decryption respectively. Of course, this procedure can only be performed properly with the accurate key.

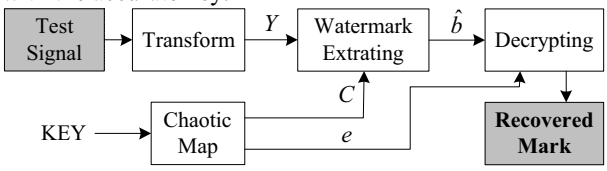


Fig. 3 Watermark extraction diagram

The test signal is commonly the received version of the watermarked signal that may suffer some attacks. Then, in the transform domain, the host signal Y can be represented as,

$$Y = \tilde{X} + V \tag{7}$$

Where, the part V is the noise introduced by the attacks including some common signal processing. Coordinates of the host data Y are also divided into two complementary sets Ψ_1 and Ψ_2, which is quite similar to (3).

Detection is performed by first computing the sufficient statistic ξ_Y :

$$\xi_Y = \frac{1}{N_1} \sum_{i \in \Psi_1} Y(i) - \frac{1}{N_2} \sum_{i \in \Psi_2} Y(i) \tag{8}$$

And estimating the embedded bit by,

$$\hat{b} = \begin{cases} 1, & \xi_Y \geq 0 \\ 0, & \xi_Y < 0 \end{cases} \tag{9}$$

Here, the bit $\hat{b}$ is regarded as the elements of the encrypted watermark data $\hat{w}_{en}(k) = \hat{b}$, $k = 0,1,\Lambda$, $L-1$.

With the help of the sequence e, the watermark is recovered by performing the decrypting calculation, $\hat{w}(k) = \hat{w}_{en}(k) \oplus e(k), k = 0,1,\Lambda\ , L-1$, where L is the length of the watermark bit sequence. Because the original image is not needed in the extracting phase, this scheme belongs to the blind watermarking family.

4. PERFORMANCE ANALYSES

As in [3-5], assume the host signal X and the processing noise V both satisfy normal distribution in our scheme. Although there are some arguments about this, it is still reasonable to accept it especially when the accurate distributions of X and V are not reachable. The Gaussian variables $X(i)$ and $V(i)$ satisfy $X(i) \sim N(\mu_X, \sigma_X^2)$ and $V(i) \sim N(\mu_V, \sigma_V^2)$. From (3), we can find that ξ is also random variable with distribution $\xi \sim N(0, \sigma_\xi^2)$, where $\sigma_\xi^2 = (1/N_1 + 1/N_2) \cdot \sigma_X^2$. Function $f(\xi)$ is used to represent the probability density function of ξ. Besides, the hidden bit is assumed to be 1 in this section to convenient the analyses.

As discussed above, the energy of the embedded watermark is controlled by the parameter Δ. We employ E_w to denote the energy embedded for each watermark bit. From (5) and (6), E_w can be formulated as,

$$E_w = (N_1 + N_2) \cdot E\left[\frac{\alpha^2}{4}\right] = N \cdot \int_{-\infty}^{\Delta} \frac{(\Delta - \xi)^2}{4} \cdot f(\xi) d\xi \qquad (10)$$

In the receiver side, the tested image Y is pollutes by V. To make a proper decision on the embedded mark bit, the statistic can be formulated approximatively as

$$\begin{aligned} \xi_Y &= \frac{1}{N_1}\sum_{i\in\Psi_1} Y(i) - \frac{1}{N_2}\sum_{i\in\Psi_2} Y(i) \\ &> \Delta + \frac{1}{N_1}\sum_{i\in\Psi_1} V(i) - \frac{1}{N_2}\sum_{i\in\Psi_2} V(i) = \widetilde{\xi}_Y \end{aligned} \qquad (11)$$

We model the statistic ξ_Y satisfying normal distribution as $\widetilde{\xi}_Y$. Though this assumption is not quite accurate, we can get a reasonable approximate performance bias by it. The mean and the variances of $\widetilde{\xi}_Y$ will be decided by $E[\widetilde{\xi}_Y] = \Delta$ and $Var[\widetilde{\xi}_Y] = (1/N_1 + 1/N_2) \cdot \sigma_V^2 = \sigma_R^2$, or formulated as $\widetilde{\xi}_Y \sim N(\Delta, \sigma_R^2)$. The error probability of the extracted watermark bit will be decided by,

$$P_e < \frac{1}{2} erfc\left(\sqrt{\Delta^2/(2 \cdot \sigma_R^2)}\right) \qquad (12)$$

5. EXPERIMENTAL SIMULATIONS

The 512×512 size 8-bits gray image "Lena" (Fig. 4(a)) acts as the host image in the simulation. Binary image "JTUMCI" (Fig. 4(b)) serves as the watermark data, whose size are 64×64 bits. Block-based DCT "Transform" is employed, though it is not constraint to in practice (DWT/DFT or Space-Time domain also fitted).

5.1. Watermark Embedding and extraction

The host image is divided into 8×8 size blocks and performed with inner-block DCT, which is coincident with JPEG and MPEG2 standards. The middle and high frequency coefficients then act as the host data to embed the encrypted mark bits as (3)-(6). The lowest 6 coefficients in each block are protected and set $N_1 = N_2 = (64-6)/2$, i.e. $N = N_1 + N_2 = 58$. ICMIC is employed to produce the chaotic sequences to perform coefficients classification and watermark encryption. The watermarked image is shown in Fig.4(d). If the watermark intensity is properly selected by controlling Δ, the visual quality of the marked image is quite good. The watermark can be recovered accurately with the authorized keys if no attack occurs, which is shown in Fig. 5(e).

(a)Original Image (d)Watermarked Image

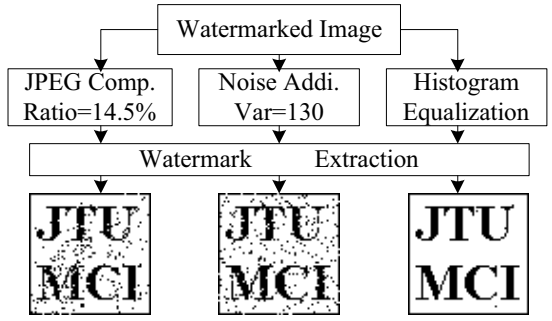
(b)Original Watermark (c)Encrypted Watermark (e)Recovered Watermark

Fig. 4 Samples during watermark embedding & extracting

5.2. Performance evaluation of the proposed scheme

Parameter Δ is adjusted to control the embedding intensity of watermark, which is reflected by peak signal-to-noise ratio (PSNR) of the watermarked image. And the bit error ratio (BER) of the extracted watermark acts as the index of the robustness of the watermarking scheme.

Attacks such as JPEG compression, noise addition and histogram equalization are performed to evaluate the robustness of our scheme as in Fig.5. PSNR of the marked



(a) BER=5. 517% (b) BER=6. 445% (c) BER=0.0977%

Fig. 5 Extracted watermark under attacks

image is set to about 41 dB to ensure the perceptual quality as in Fig. 4(d). The watermarked image is compressed (JPEG) to 14.5% of its original size (from 257KB to 37.5KB) and the BER of the extracted watermark is 0.05517, in Fig. 5(a). After severe Zero-mean Gaussian noise addition (whose variance is 130), the PSNR of the polluted image is only 26.97dB and the visual quality is awful. However, the extracted watermark is still readable (BER=0.06445) as shown in Fig 5(b). Finally, histogram equalization is performed on the watermarked image and the extracted watermark is shown in Fig. 5(b), which indicates that our scheme has high robustness to this kind of luminance transforms.

Besides, objective comparisons with the SS scheme [4] are presented in Fig. 6. In the employed SS scheme [4], the spread watermark is embedded into middle-high frequency coefficients of image blocks in block-based DCT domain, where the block is 8×8 size and 64×64 bits watermark data are embedded in the same coefficients of image "Lena". This scheme was regarded as with high robustness to compression (JPEG) and noise addition [5]. To these two schemes, the BER curves of the

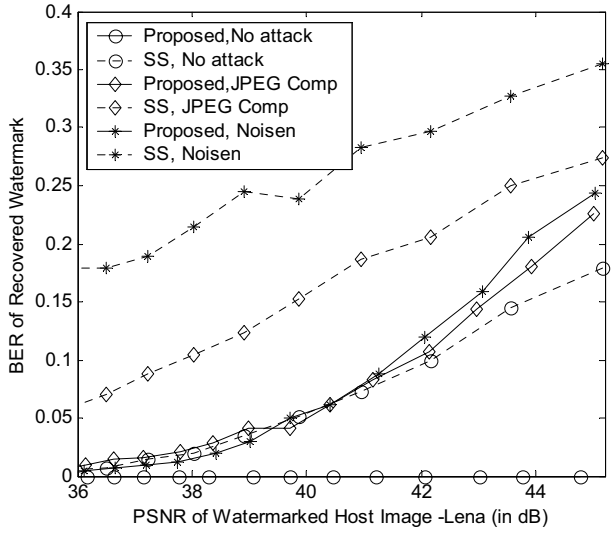


Fig. 6 Experimental comparisons with SS scheme in [4]

extracted watermark are different to each other under the same level of JPEG compression (ratio 14.5%) and Gaussian noise (variance130) addition. The BER curves descend more rapidly than that of SS scheme [4] when the intensity (reflected by PSNR of the watermarked image) of the watermark increases. It is obvious that the BER of our scheme is much lower than that of the traditional SS in each similar condition. If no attack occurs, the BER of the extracted mark in our scheme is zero even when the watermark intensity is low. However, the BER of the watermark in the SS scheme increases as the decrease of the embedded watermark intensity because the image signal is regarded as noise to watermark signal [4,5].

6. CONCLUSIONS

The projects of designing reliable watermarking for multimedia copyright protection require sustained technical innovations on this front. The introduced algorithm is non-additive with good balance between the requirements such as *imperceptibility*, *robustness* to attacks and *security* for the common robust watermarking schemes. Comparisons with the more mature spread spectrum watermarking schemes [4] and rich experimental results have also proved its validity.

7. ACKNOWLEDGEMENT

This research was supported by Hi-Tech R&D Program of China No. 2002AA144110 and Natural Science Foundation of China under Grant No. 60272082.

8. REFERENCES

[1] Sin-Joo Lee; Sung-Hwan Jung: "A survey of watermarking techniques applied to multimedia," IEEE Proc. Of the ISIE Vol. 1, pp. 272 –277, 2001

[2] Di He, Chen He, Ling-ge Jiang, and ect., "Chaotic Characteristics of a One-dimensional Iterative Map with Infinite Collapses," IEEE Transactions on Circuits and System-IVol.48, No.7, pp. 900-906, July 2001.

[3] Cox I.J., Kilian J. and etc.: "Secure spread spectrum watermarking for multimedia [J]," IEEE Transactions on Image processing, Vol. 12, No. 6, pp. 1673~1687, 1997.

[4] Hernandez J.R., Amado M. and etc., "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," IEEE Trans on Image Processing, Vol. 9, Is. 1, pp: 55-68, Jan. 2000.

[5] Malvar H.S. and Florencio D.A.F., "Improved spread spectrum: a new modulation technique for robust watermarking," IEEE Transactions on Signal Processing, Vol. 51, Is. 4, pp. 898 –905, Apr. 2003.

[6] Furon T. and Duhamel P., "An asymmetric watermarking method," IEEE Transactions on Signal Processing, Vol. 51, Is. 4, pp. 981-995, Apr. 2003.