Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 3 Özel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 3 Special Issue (2015)
ISSN: 1300-1949

A robust video watermarking algorithm based on chaotic maps and discrete wavelet transform

Somayyeh MOHAMMADİ[1,*]

[1,] *Department of Engineering Payame Noor University, Kerman, Iran*

Received: 01.02.2015; Accepted: 05.05.2015

Abstract. In this paper, we present a video watermarking scheme based on chaotic maps in wavelet domain. The embedding procedure is done before video compression stage. At first, we encrypt the watermark signal by a Tent map, next the encrypted watermark is embedded in HH sub-band coefficients of I-frames. This task will increase the security and resistance of our watermarking system. Experimental results verify the resistance of our proposed method against signal processing and geometric attacks. We also comprise the efficiency of our algorithm against some other methods. Comparison results show the superiority of our scheme against others.

Keywords: Watermarking, Chaotic maps, Discrete wavelet transform, Robustness, Security.

1. INTRODUCTION

However internet networks expansion makes distributing and transforming of multimedia data easily but it causes owners to be worry about fake or illegal distribution of their properties. Up to now some solutions have been suggested to prevent illegal distributions. Among them digital watermarking is an effective way to maintain digital multimedia data from illegal distribution.

To design a digital watermarking scheme, considering of some factors that rise method efficiency, is a necessity. Robustness, transparency, capacity, security, and simplicity are some of these factors. Watermarking algorithms can be categorized in two groups: blind and non-blind. Methods which don't need the original host signal in the extraction stage place in blind class and the others that need the original host signal to extract the watermark signal, belong to non-blind group. A large number of watermarking algorithms are presented in image [1, 2] and video fields [3, 4]. Of course lack of security is a problem which involved researchers to have more secure methods. This intention leads to use chaotic maps in watermarking systems [5]. Since chaotic maps have an intensive dependency on their initial values and they are non-periodical, researchers are interested using these sequences in their watermarking algorithms. Although there is some watermarking methods based on chaotic maps but most of them are about images [5-7] and a few of them are related to video issues [8].

*Corresponding author. *Email address*: *s_mohammadi@pnu.ac.ir*

Special Issue: The Second National Conference on Applied Research in Science and Technology

As we know each video frame consists of a number of consecutive frames. Typically there is a high correlation between pixels whose place in a frame or adjacent frames, so a video stream has large redundancy. Attending to this fact, actuate researchers to compress video signals before restoring or sending through internet [9]. The idea in compression procedure is to omit or decrease spatial and time redundancies. Spatial redundancy is for correlation between inner pixels and time redundancy is for correlation between pixels in a frame with neighbor frames. By transforming a frame from one domain to another domain, we can decrease the spatial redundancy and applying motion estimation and compensation algorithm will reduce the time redundancy. In MPEG2 compression standard, frames are coded in two ways: intra and inter. In intra coding, the frame is coded and sent without using motion estimation and compensation algorithm while in inter coding, the deference of current frame with previous or next frame is coded and sent. According to this, there are three types frames in MPEG2 standard named I, P, and B. I-frames are be coded as intra, P and B-frames are coded as inter. It is noticeable to say that the reference frame for P-frames is from I groups while for B-frames is from I or P groups.

By considering of compression stage, watermarking algorithms can be put in two classes based on compression or non-compression domain. Watermarking methods based on compression domain execute the watermark embedding, next or at the time of compressing, whereas in non-compression methods, the watermark signal is embedded before compressing the video stream.

The proposed method in [3] is a technique based on singular value decomposition (SVD) which done in discrete wavelet transform (DWT) domain. The presented watermarking algorithm in [4], embeds the watermark signal before compression stage, in this method the watermark is hidden in wavelet coefficients reached after two decomposition levels. Writer's reason of choosing two decomposition levels is enjoying good resistance as well high transparency. Researchers in [10] first divide the original video into groups of pictures with a fixed number of frames. They then compute the 1-Dimensional (1-D) discrete Fourier transform along the temporal direction of each GOP and finally choose the highest temporal frequencies to embed the watermark in the Radon transform of selected frames. This technique has tolerable resistance, nevertheless using two transform makes it, more complicate.

The main concentration of this study is the utilizing of chaotic maps and DWT to design a good video watermarking system. The embedding procedure is implemented before video compression stage. In order to have a more secure method, we encrypt the watermark signal by a chaotic map called Tent map. The resistance of our proposed algorithm is increased with using of DWT. We select the luminance component (Y-component) of I-frames as embedding positions. Of course, in this scheme the DWT is applied in one decomposition level and we modify some coefficients of HH sub-band. Since in our proposed method, the watermark embedding stage is before video compression, so our method is not dependable to any specific compression standard. However it is possible to anguish about maintaining of watermark after applying compression stage, because each compression standard includes of quantization level. This function will attend to removing some information. The simulation results show that our proposed method has good resistance against JPEG compression. We consider our video watermarking for MPEG2 standard.

The rest of this paper is organized as follows:

In section 2, we describe chaotic maps briefly. The algorithm is presented in section 3. In section 4, simulation and comparison results are brought. Finally, we conclude our study in section 5.

2. CHAOTİC MAPS

Chaotic maps are sequences which resulted from non-linear chaotic systems. These sequences are pseudo random sequences that some their significant properties are: dependency to seeds, non-periodical, and non- predictable [11]. There are varieties of chaotic maps with different dimensions. For example, we can point to: Tent map, Kaplan-Yorke map, and Logistic map.

Tent map is an 1-D chaotic map that introduced by (1): [5]

$$\begin{aligned} x_{n+1} &= a x_n \quad for\, 0 \le x \le 0.5 \\ x_{n+1} &= a(1 - x_n) \quad for\, 0.5 \le x \le 1 \end{aligned} \tag{1}$$

Where a, is the chaotic parameter ($0 < a \le 2$) and n is the iteration number to construct this sequence. The Kaplan-Yorkemap map is built by (2): [5]

$$\begin{aligned} x_{n+1} &= a x_n \bmod 1 \\ y_{n+1} &= b y_n + \cos(4\pi x_n) \end{aligned} \tag{2}$$

In this relation "mod" means remainder, a, and b are chaotic parameters *(0≤a≤2, 0≤b≤1).* The Lyapunov exponent is a parameter which introduced for chaotic maps. To describe this parameter it is first necessary to be familiar by Lyapunov number $L(x_1)$ that brought in (3): [11]

$$L(x_1) = \lim_{n\to\infty}\left(\left|f'(x_1)\right| \ldots \left|f'(x_n)\right|\right)^{1/n} \tag{3}$$

Where *f(.)* is the chaotic function and n is the iteration number to construct the map. So the Lyapunov exponent $h(x_1)$ is [11]:

$$h(x_1) = \lim_{n\to\infty} \left(1/n\right)\left[\ln\left|f'(x_1)\right| + \ldots + \ln\left|f'(x_n)\right|\right] \tag{4}$$

For each chaotic map (4) is zero.

In this paper, we encrypt the watermark signal by a Tent map. As this sequence is sensitive to its seed, so the initial value consider as a key. The chaotic parameter is another key. If a chaotic map has had high dimensions, the number of chaotic parameter and seeds would be increased and in continue the watermarking system would be more secure.

3. THE PROPOSED METHOD

We embed the watermark bits in luminance parts (Y- component) of I-frames. Of course we apply DWT in one decomposition level on Y-component. To design a watermarking method, we should attend to collusion attack. In this attack [12] the attacker can estimate the watermark by averaging of frames and alters or removes the watermark. So a watermarking algorithm will be vulnerable against this attack when the same watermarks are embedded in different frames or different watermarks are embedded in too similar frames [12].

In our proposed method in this study, in order to resist against this attack, we produce different watermarks for each distinct I-frame. We consider our proposed technique for MPEG2 standard. But as stated in introduction section, since watermark embedding stage is done before compression stage, and then our algorithm is undependable of compression standard type. To explain our method in details, we describe watermarking procedure in three phases.

Phase 1: in this phase, we encrypt the watermark signal which is a binary logo by using (1). We go the encryption procedure as bellow:

-Construct the Tent map by (1). (Note: this sequence gives us decimal numbers [0-1]).

- Convert resulted numbers from (1) to -1 and 1 by (5). (Produce a bipolar sequence)

$$x_{n,new} = round(x_n) \quad n = 1,\ldots,N$$

$$x_{n,bipolar} = \begin{cases} 1 & x_{n,new} = 1 \\ -1 & x_{n,new} = 0 \end{cases} \tag{5}$$

Where x_n is the constructed chaotic map by (1) and N is the number of watermark signal bits.

- Reshape the watermark logo (w) to a vector. Then change it to a bipolar sequence via (6):

$$w_{n,bipolar} = \begin{cases} 1 & w_n = 1 \\ -1 & w_n = 0 \end{cases} \quad n = 1,\ldots,N \tag{6}$$

-Now, we reach to an encrypted watermark signal by (7):

$$w_{encrypt} = w_{bipolar} \times x_{bipolar} \tag{7}$$

As we have pointed at the fist of this section, in order to have good resistance against collusion attack, we build different watermarks for each frame. To build different watermarks, it is enough, to change only the initial value of chaotic map, because these sequences are extremely sensitive to their seeds. And also to prevent of sending large information, we define seeds as (8):

$$x_0(i) = \frac{x_0(i-1)}{m}, \quad i = 2,..,m \tag{8}$$

Where m and $x_0(1)$ are the frame index and initial value of first frame, in that order. It is noticeable to say that in this stage, the seed and chaotic parameter of (1) are keys which without knowledge of them in extraction stage, the extraction will be very difficult.

Phase 2: This step is called watermark embedding. We select y-components of I-frames as embedding positions; the embedding procedure is performed before compression stage and in transform domain. The DWT is applied in one decomposition level and the HH sub-band is considered as embedding region (Figure. 1.). It is better to summaries embedding procedure in following steps:

Step 1. Put HH sub-band's coefficients in a B1 collection at descent order. (The first number in this collection has the maximum value among HH coefficients).

Step 2. Put HH sub-band's coefficients in a B2 collection at ascent order. (The first number in this collection has the minimum value among HH coefficients).

Step 3. Separate coefficients from B1 as same as the number of available '1's in the encrypted watermark and put them in a new collection called B3.

Step 4. Separate coefficients from B2 as same as the number of existing '-1's in the encrypted watermark and put them in a new collection called B4.

Step 5. Apply the embedding procedure by (9).

$$\begin{cases} \overline{b}_{i,3} & if\ w_{i,encrypt} = 1 \\ b_{i,4} & if\ w_{i,encrypt} = -1 \end{cases} \quad i = 1, 2, 3, ..., N \tag{9}$$

Where $b_{i,3}$ and $b_{i,4}$ are the least significant bits (LSB) of B_3 and B_4 collections respectively. $W_{i,encrypt}$ is the encrypted watermark and N is the number of watermark bits. Furthermore in this relation $\overline{b}_{i,3}$ is the complementary value of $b_{i,3}$. Note: we should save the layout of coefficients in B_3 and B_4. Because we detect the watermark signal at extraction phase based on this layout. After completion of these steps, apply the inverse DWT (IDWT). Thus the watermarked frame will be achieved.

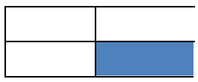

Figure.1. The embedding region (the colored zone).

Phase 3. In this phase, our aim is the extraction of watermark from video stream. At first, we apply DWT in one decomposition level on Y-components of I-watermarked frames. Do the steps 1-4 from previous phase. Then by accomplishing of (10), the watermark signal (w') will be obtained.

$$w'_i = \begin{cases} 1 & if\ B_{i,3} > 0 \\ 0 & if B_{i,4} < 0 \end{cases} \quad i = 1, 2, 3, ..., N \tag{10}$$

Where $B_{i,3}$ and $B_{i,4}$ are coefficients in B_3 and B_4 collections, respectively.

4. SİMULATİON RESULTS

In this section, we are brought the simulation results of our proposed scheme and as well comparison results against the proposed method in [10].

Evaluation results

The simulation is done in MATLAB simulator. We encrypt watermark signal according to the description in section 3. We test our algorithm on Pedestrian video (720×576 resolution).in this study, we are written the results related to the first I-frame. The initial value and the chaotic parameter are set as 0.01 and 1.75, respectively. Figures. 2a and 2b, are shown the original and watermarked frame and also the original and encrypted watermark logo are illustrated in Figures. 2c, and 2d, respectively. The transparency quantity is evaluated by PSNR (Pick Signal to Noise Ratio) criteria (equation (11)). According to this value and Figure.2b, we see the proposed algorithm can well hide the watermark in the original signal as it is not observable by human eyes.

$$PSNR = 10\log((255\verb|^|2)/MSE)$$
$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}\left|X(i,j) - X^{'}(i,j)\right| \tag{11}$$

Where X and X' are the original and watermarked frames correspondingly.

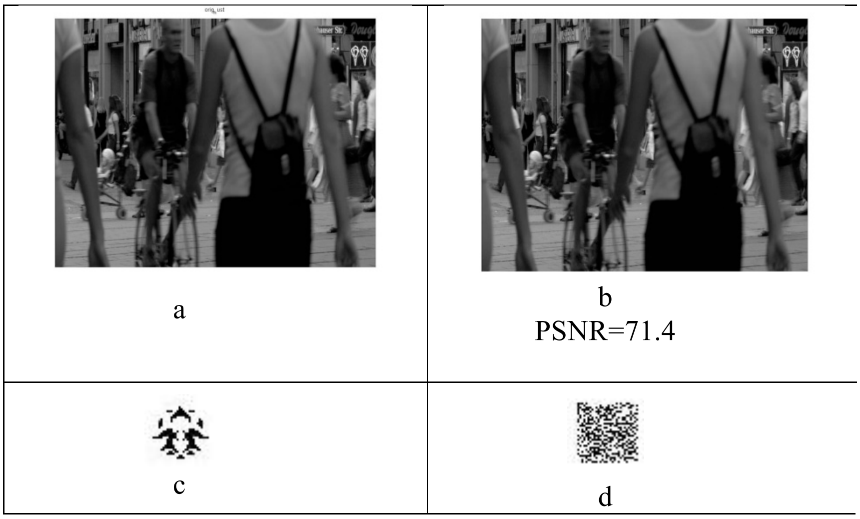

Figure 2. a) The original frame, b) The watermarked frame, c) The original watermark, and d) The encrypted watermark.

The robustness results of our proposed algorithm are briefed in Table 1. We calculate the wrong extracted watermark signal bits by BER (Bit Error Rate) measurement.

$$BER = \frac{B}{m} \tag{12}$$

Where B is the erroneous extracted bits and m is the watermark's length. It is inferred from this table that our method has a good resistance against JPEG compression in different QFs (Quantization Factors). Against rotation attack, it has also excellent vulnerability. We test the robustness of our method against salt & pepper noise and some kinds of filters as well. It can be seen from results in Table 1, that the proposed watermarking system has a good ability to extract watermark even after applying these attacks.

Table 1. BER results and extracted watermarks after applying some attacks.

Attacks	BER	Extracted Watermarks
No attack	0.00	
Salt & Pepper Noise (0.001)	0.03	
Gaussian Noise (0.001)	0.25	
Median [3 3]	0.21	
Median [2 2]	0.14	
Gaussian Filtering	0.00	
Wiener Filtering	0.05	
JPEG (QF=95)	0.02	
JPEG (QF=85)	0.10	
JPEG (QF=70)	0.17	
Rotation (1^0)	0.01	
Rotation (3^0)	0.02	
Rotation (7^0)	0.07	

Comparison Results

In order to illustrate the efficiency of our proposed scheme, in this part we do a comparison between our proposed method and method in [10]. The comparison diagram is shown in Figure. 3. In this figure, vertical axis is "sim". Sim means the similarity between the original watermark and extracted one, which is calculated by (13) and horizontal axis is the attack applied to watermarking system.

$$sim = \frac{\nabla w' \times \nabla w^T}{\sqrt{\left(\nabla w' \times \nabla w'^T\right)\left(\nabla w \times \nabla w^T\right)}} \tag{13}$$

In this formula, w is the original watermark signal, w' is the extracted watermark, ∇ means gradient, and *T* symbol means transpose. It can be conceived from Figure. 3, that "sim" value is very near to "1" for our presented method in this study against [10] which shows the superiority resistance of our algorithm to [10].

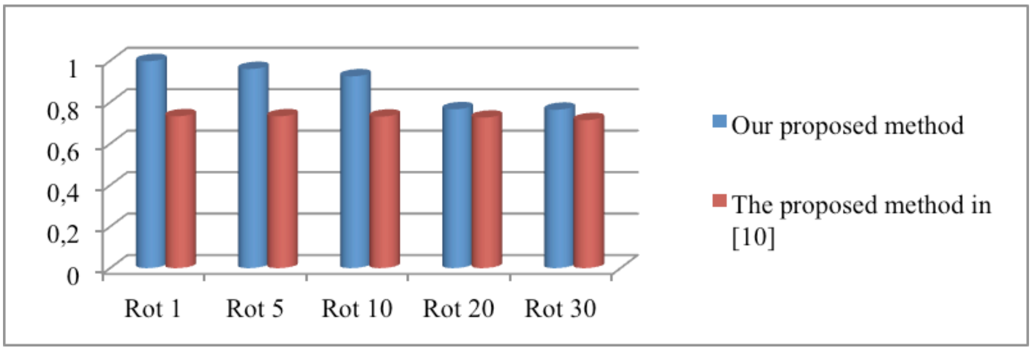

Figure 3, Comparison results.

5. CONCLUSİONS

In this paper, the aim is enjoying of remarkable features of chaotic maps in designing of a secure watermarking algorithm. In this method, the encrypting of watermark signal is done by companionship of chaotic maps. We embed the watermark in DWT domain. In MPEG2 compression standard, I-frames is compressed fewer, hence selecting of these frames as embedding positions are more suitable related to P and B-frames. We evaluated the robustness of our algorithm against to some usual attacks. We also comprised the performance of our proposed method with [10]. The comparison results show the supremacy of our scheme to the proposed method in [10].

REFERENCES

[1] Xinge You, Liang Du, Yiu-ming Cheung, and Qiuhui Chen. (2010), "A blind watermarking scheme using new nontensor product Wavelet filter banks, " IEEETransactions on image processing, vol. 19, no. 12, December.
[2] Chandra Mohan B and Srinivas Kumar S. (2009), "Roubust Multiple Image Watermarking Scheme using Discrete Cosine Transform with Multiple Descriptions," International Journal of Computer Theory and Engineering ,Vol. 1, No. 5, pp. 1793-8201, .
[3] Osama S. Faragallah. (2013), "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," Int. . Electron. Commun. (AEU) 67, pp.189-196.
[4] Radu O. Preda and Dragos N. Vizireanu. (2010), "A robust digital watermarking schem for video copyright protection in the wavelet domain. " Measurement 43 pp.1720-1726.

[5] Narendra Singh, Aloka Sinha. (2010), “Digital image watermarking using gyrator transform and chaotic maps,” ,Optic 121, pp. 1427-1437.
[6] Z. Yuxia, F.Jingbo. (2012), “A double- function digital watermarking algorithm based on chaotic system and LWT, ” PhysicsProcedia 33. pp.1947-1956.
[7] G. Guang, J. Guo-ping. (2011), “Zero-bit watermarking resisting geometric attacks based on composite-chaos optimized SVR model, ” the Journal of China Universities of Posts and Telecommunications, 18(2):94-101.
[8] S. Chen, H. Leung. (2008), “Chaotic watermarking for video authentication in surveillanc applications,” IEEE Transactions on circuits and systems for video technology,vol. 18, no. 5.
[9] M. Ghanbari. (2003), “IEE Standard Codecs Image Compression To Advanced Video Coding eBook-LiB, ”.
[10] Y. Liu, J. Zhao. (2010), “A new video watermarking algorithm based on 1D DFT and Radon transform, ” Signal Processing 90, pp. 626-639.
[11] Kathleen T. Alligood, Tim D. Sauer and James A. Yorke. (2001), “Chaos: An Introduction to Dynamical systems”. Springer, New york.
[12] G. Doerr, Jean-Luc Dugelay. (2003), “A guide tour of video watermarking” , Signal Processing: Image Communication 18, pp. 263-282