The ISC Int'l Journal of Information Security
ISeCure

January 2012, Volume 4, Number 1 (pp. 77–86)
http://www.isecure-journal.org

A Chaos-Based Video Watermarking Algorithm ☆

Somayyeh Mohammadi [1,*] and Ahmad Hakimi [1]
[1] *Department of Electrical Engineering, Shahid Bahonar University of Kerman, Kerman, Iran*

ARTICLE INFO.

Article history:
Received: 3 November 2011
Revised: 26 January 2012
Accepted: 27 January 2012
Published Online: 30 May 2012

Keywords:
Chaotic Maps, Robustness, Security, Watermarking

ABSTRACT

The intriguing characteristics of chaotic maps have prompted researchers to use these sequences in watermarking systems to good effect. In this paper we aim to use a tent map to encrypt the binary logo to achieve a like-noise signal. This approach makes extraction of the watermark signal by potential attacker very hard. Embedding locations are selected based on certain principles. Experimental results demonstrate that our proposed watermarking method is highly superior to other techniques reported in literature and readily achieves the desired robustness and security level.

1 Introduction

Recently, with exorbitant growth of Internet networks and multimedia technology such as image, voice, and video information exchanges we are increasingly witnessing transition and distribution of these data through Internet. Therefore, there is a growing concern that we may encounter illegal distributions.

Digital watermarking is a good technique to prevent illegal distributions of multimedia data. Although there are a variety of digital watermarking methods [1–3], but the performance of any digital watermarking must be evaluated on merits such as: transparency, robustness, capacity, security, and rapid detection. In a good watermarking algorithm, the watermark that has been inserted into the host signal should be invisible by the human eye.

Usually each watermarked signal may be subjected to intentional or unintentional attacks where the signal is chased and an attempt is made to alter or remove the watermark from the watermarked signal. Filtering, adding noise, and geometric distortions are among these attacks [4].

With video content there is another main attack called collusion attack [5, 6]. This attack applies when there is the same watermark in a number of different frames or when there is a different watermark in a number of identical frames. To counter this kind of attack, the watermark inserted into two different frames of a video signal should be as identical in terms of correlation as the two frames are. Capacity defines the amount of bits that we can hide in the host signal.

Another important parameter which manifests itself in a superior performance watermarking technique is security. Security is related to keys which are used in an embedding stage, so that the more the keys the securer the method [7]. Rapid detection refers to the ability to detect watermark within a small number of frames ideally from each single frame in isolation. This factor for real time videos is vital. Since there is a trade-off between these different factors, we should keep a factor in an ideal level based on method's application.

Most of digital watermarking methods suffer from low security of their watermarking systems. Recently, due to noticeable properties of chaotic maps, they are used in the secure communication systems as well as watermarking systems [8, 9]. Some of the properties of such system are sensitivity to the initial conditions

☆ This article is an extended/revised version of an ISCISC'11 paper.
* Corresponding author.

Email addresses: mohammadi_0313@yahoo.com (S. Mohammadi), hakimi@mail.uk.ac.ir (A. Hakimi).

ISSN: 2008-2045 © 2012 ISC. All rights reserved.

and not being periodical. Most of recent proposed watermarking methods based on chaotic maps are for watermarking of images [8, 10–12] and a few methods have been proposed for video applications [13].

In this paper [1], we focus on applications of chaotic maps for video watermarking [14]. We encrypt a binary watermark into a tent map [8], to have a like-noise signal. This approach makes extraction and detection of watermark durable for attackers.

All video watermarking methods are categorized into two domains: uncompressed domain [15–19] and compressed domain [20, 21]; in which the uncompressed domain can in turn be divided into spatial domain [19] and transform domain [15–18]. Methods based on uncompressed domain are independent of compression standard being applied whereas in our study we regard compression as an attack. Therefore, the model we develop must be robust enough against all compression attacks. The main advantage of working in spatial domain is its simplicity and its low computational complexity which are characteristics attractive for video watermarking.

Since our proposed method also embeds the watermark in spatial domain, the results in Section 5 verify its robustness for JPEG compression.

The video watermarking algorithm in [15] first divides the original video into groups of pictures (GOP) with a fixed number of frames. It then computes the 1-Dimensional (1-D) discrete Fourier transform along the temporal direction of each GOP and finally chooses the highest temporal frequencies to embed the watermark in the Radon transform of selected frames. The proposed method in [16] deals with uncompressed videos in the Wavelet domain, where the watermark is embedded in the Wavelet coefficients of the second Wavelet decomposition level. The Authors claim the choice of the second decomposition level is a tradeoff between the invisibility of the watermark and the resilience to attacks. In [17] researchers present a video watermarking algorithm based on full DCT domain. The reasons given for using full DCT is to minimize the embedding complexity as well as to get rid of spatial synchronization.

In [22], the scale invariant feature transform is used to generate circular patches as the embedding units. In [23], the watermark is embedded into rotation and scaling (RS) invariant regions which were obtained by adopting log-polar mapping and 2-D discrete furrier transform. In this scheme, for resisting different video format conversions, the watermark detection is performed in the spatial domain along with video playing. The proposed method in [24] is a DCT based method that the addition of the watermark to the quantized DCT coefficients is the addition of the watermark times the quantization step size to the original DCT coefficients.

In general, we can utilize chaotic maps in a watermarking scheme as follows:

- To generate the watermark.
- To encrypt the watermark.
- To scramble the host signal.
- To have a randomly distribution of the watermark bits around the host signal.

The proposed method in [25] has increased security of its watermarking method due to use of chaotic maps. In this method, watermark is hidden in a chaotic structure and the watermarking method is performed based on the bit-zero watermarking algorithm [26]. In [27], two chaotic maps are employed: one map for disturbing the host image and another map to obtain a scrambled watermark. In fact, by using an exclusive-or operation between a chaotic image pattern obtained by a logistic map and the binary watermark, the scrambled watermark will be reached.

The watermarking scheme in [8] encrypts a watermark signal by multiplying the watermark by some chaotic maps. Namely, the like-noise watermark will be embedded in the host image. In [10], the embedding positions are chosen by using a chaotic map. This kind of selection will improve the robustness of the watermarking algorithm against some attacks.

Since in our proposed method watermark signal is embedded in spatial domain and before video compression, our method is not dependent on any particular video compression standards. However, our method may be protective against compression, because video compression standards require quantization which results in information loss. Simulation results demonstrate resistance of our proposed watermarking system against JPEG compression. We consider the proposed method for MPEG-2 video.

The rest of the paper is organized as follows. Section 2 introduces the MPEG-2 standard. In Section 3 we take a look at chaotic maps and present our proposed method in Section 4. The experimental results verifying the robustness of this enhanced technique together with a comparison of its features against the newest method is presented in Section 5. The paper in its concluding section outlines the advantages of the proposed technique highlighting its resiliency and potentials to overcome many key challenges that face watermarking systems including security and cumbersome computational requirements.

[1] An earlier version of this paper has been presented and published at the 8th International ISC Conference on Information Security and Cryptology [14].

2 MPEG-2 Standard

Each video sequence is consisted of ordered frames, where in each frame and between ordered frames hard correlation exists. Inter-frame correlation, which is called spatial redundancy, can be reduced using mathematical transforms such as Discrete Cosine Transform (DCT). The intra-frame correlation is called temporal redundancy and can be reduced by motion estimation and motion compensation. Therefore, compression is required for transmission and storage of video [28].

Compression means reduction of information while keeping quality of video. In compression of video for transmission, we are working on coding and decoding of video, which are performed by coder in transmitter and decoder in receiver respectively.

In MPEG-2 standard [28], frames are coded in three forms which are I, P and B. In I-frames, focus is on omitting of spatial redundancy. While the P and B-frames also work on omitting of temporal redundancy. Since in ordered frames, few object movements are performed, it is possible to avoid redundant information by prediction of current frame using previous or next frames.

In P-frames coding, current frame is predicted from the previous one. This is while in B-frames it is more possible to omit correlated information, Since in coding of these frames, the current frame prediction is based on the movement of previous or next frame. This approach reduces mass of transmitted video significantly. However, such frames have lower quality than the other frame types.

In general, we comprise the frames types from compression rate aspect as follows:

B-frame → P-frame → I-frame

And from quality view point:

I-frame → P-frame → B-frame

In a watermarking system, we encounter host signal distortion. As to embed the watermark signal in the host signal, it is necessary to make some alterations in the host signal, which reduces quality of this signal.

Based on this fact, and compression properties of different frame types in MPEG-2, we have chosen I-frames for watermark embedding position. This kind of selection will preserve the quality of watermarked video sequence while protecting it against watermark removing attacks, because because removal of I-frames causes quality reduction of video sequence.

3 Chaotic Maps

Chaos identifies itself with non-periodicity, a phenomena which is sensitively dependent on initial conditions [29]. Dependence on initial conditions refers to the property that pairs of points “which begin as close together as desired” will eventually move apart, since the chaotic orbits separate exponentially fast from their neighbors as the map is iterated.

Chaos is defined by a Lyapunov exponent greater than zero. The Lyapunov number is the average per step divergence rate of nearby points along the orbit and the Lyapunov exponent is the natural logarithm of the Lyaponov number. Next, we formally describe these concepts in terms of mathematical relationships. Suppose f is a smooth map of the real line R. The Lyapunov number $L(x_1)$ of the orbit $\{x_1, x_2, x_3, \ldots\}$ is defined as [29]:

$$L(x_1) = \lim_{n\to\infty} (|f'(x_1)| \ldots |f'(x_n)|)^{\frac{1}{n}} \quad (1)$$

if this limit exist. Also the Lyapunov exponent $h(x_1)$ can be defined as:

$$h(x_1) = \lim_{n\to\infty} \left(\frac{1}{n}\right) [ln|f'(x_1)| + \ldots + ln|f'(x_n)|] \quad (2)$$

if this limit exists. Notice that h exists if and only if L exists and it is nonzero and $ln(L) = h$.

In this paper the chaotic map which we use is the tent map. The tent map with slope a is given by [29]:

$$T_a(x) = \begin{cases} ax, & \text{if } x \leq \frac{1}{2} \\ a(1-x), & \text{if } x \geq \frac{1}{2} \end{cases} \quad (3)$$

This map is continuous but not smooth because of the corner at $x = 1/2$. In the case of the slope 2 tent map $(a = 2)$, the unit interval $I = [0, 1]$ is mapped onto itself by $T_2(x)$. In the case in which $0 < a < 2$, the tent map has a single fixed point at 0. For $a > 1$, the complement of I maps onto the complement of I. Therefore, if a point x is mapped outside of I, further iteration will not return it to I . For $1 \leq a \leq 2$, the points of I stay within I. For $a > 2$ most of the points of the unit interval eventually leave the interval on iteration, never to return.

4 The Proposed Method

We dedicate our method to MPEG-2 standard, but since watermark embedding is performed in spatial domain this method is independent of any compression standard and can be applied to all video compression standards. However, we still need to confirm that our method is robust with respect to these compression standards because the compression operates like an attack. The experimental results in the next section demonstrate that robustness is assured with this innovative scheme. Although the existence of I-frames is essential in video signals but despite their presence these frames are compressed to somewhat lower degree than P-frames and B-frames. So we select Y components of I-frames as embedding positions.

In order to survive collusion attacks, we embed different watermarks in each I-frame. In order to generate watermarks, we multiply a binary logo image by a tent map and then for each frame we change the seed of the tent map. Hence, this is how we can generate different watermarks. Also for sending low seeds as watermarking system keys, we choose seeds which are proportional to frame's number. The proposed method is as follow:

4.1 Watermark Generation

The watermark signal can be considered as a binary pseudo-random sequence produced by a chaotic sequence or as a binary logo image. In our proposed scheme, we have considered the watermark signal as a binary logo image.

To increase the security of our watermarking algorithm, the watermark signal is encrypted by a chaotic sequence $f(x_n)$. It is appropriate to describe the watermark generation procedure in more details as follows:

We construct a chaotic sequence by a tent map which is defined as [8]:

$$\begin{aligned} x_{n+1} &= ax_n && \text{for } 0 \le x \le 0.5 \\ x_{n+1} &= a(1-x_n) && \text{for } 0.5 \le x \le 1 \end{aligned} \tag{4}$$

where $0 < a \le 2$ and n is the iteration number. We select the seed for this chaotic map from:

$$x(0) = \frac{m}{100} \tag{5}$$

where m is the frame's number. Now we convert (4) to a bipolar sequence as:

$$x_{n,new} = 2(round(x_n)) - 1 \tag{6}$$

where x_n is chaotic sequence constructed from (4) and $x_{n,new}$ is the resulting bipolar sequence that includes -1 or 1. Our concern here is to encrypt the binary logo image in (6). Consider the binary logo as a matrix called $g(x, y)$. We convert $g(x, y)$ to a bipolar one dimensional sequence as $g(X)_{new}$, and multiply it by (6), as follows:

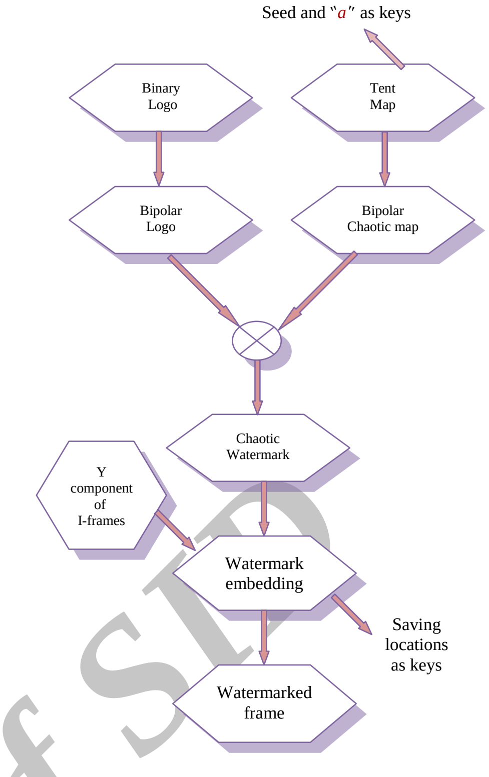

Figure 1. Block diagram of watermark embedding

$$\begin{aligned} g(X)_{new} &= 2(round(g(x,y))) - 1 \\ w(x) &= g(X)_{new} * x_{n.new} \end{aligned} \tag{7}$$

The resulting sequence called $w(x)$ is the chaotic watermark and constitutes a like-noise signal. Of course, to embed $w(x)$ into Y components, we have to make changes to $w(x)$. We elaborate how this is done in the next sub-section. Note that the number of iterations (n) corresponds to the size of the logo image.

4.2 Watermark Embedding

We select the Y components of I-frames as embedding positions to embed the generated watermark sequence from the previous sub-section. The block diagram of watermark embedding process is shown in Figure 1.

As we know, the embedding process inevitably leads to some distortions in the host signal. Therefore, high transparency is one of the most important requirements in a watermarking system. Given this challenge, our effort is to preserve the quality of the watermarked signal at a desirable level so that the eye cannot realize the existence of the watermark signal.

In our proposed method, to have a high transparency we dedicate some values proportionate to the luminance value of the host frame to the chaotic watermark by a certain principle, which we will explain in more details.

The watermark embedding is performed in spatial domain and the steps are as follows:

- First, we decompose an I-frame to its Y, U, and V components and then select the Y component.
- We search among the Y component to find two pixels whose their luminance has more repetition over this I-frame. We call these two luminance values as β_1 and β_2 so that $\beta_1 < \beta_2$, and save these locations as keys.

Obtaining β_1 and β_2 on this basis ensures that a high capacity is available in our watermarking scheme. In fact, finding values that are repeated many times make extra positions available for embedding further watermark bits.

Capacity of the proposed method is equal to the number of places with luminance values β_1 and β_2 . To increase the capacity of our proposed watermarking algorithm, it is possible to use places with luminance values close to β_1 and β_2 values as the extra embedding positions.

Now we dedicate β_1 and β_2 to the chaotic watermark as bellow:

$$w(x)_{new} = \begin{cases} \beta_1 - \varepsilon & \text{if } w(x) = -1 \\ \beta_2 - \varepsilon & \text{if } w(x) = 1 \end{cases} \tag{8}$$

where $w(x)$ is the chaotic watermark and $w(x)_{new}$ is the modified watermark that we call it, as watermark, briefly. In order to have more resilience to attacks such as image processing, the magnitude size of distance between β_1 and β_2 should be reasonable so that it can be obtained by experiment.

The ε is also a non-negative integer number. Therefore, in order to have a high degree of transparency, this number should not be very large. From the experiment, it is concluded that the best choice for ε is 3. By considering ε only for one term of (8), as found in (9) or (10), transparency will be increased.

$$w(x)_{new} = \begin{cases} \beta_1 - \varepsilon & \text{if } w(x) = -1 \\ \beta_2 & \text{if } w(x) = 1 \end{cases} \tag{9}$$

Or,

$$w(x)_{new} = \begin{cases} \beta_1 & \text{if } w(x) = -1 \\ \beta_2 - \varepsilon & \text{if } w(x) = 1 \end{cases} \tag{10}$$

In fact, using (8), (9) or (10) we convert the bipolar chaotic watermark $w(x)$ into a sequence $w(x)_{new}$ comprising $[\beta_1 \text{ or } \beta_1 - \varepsilon, \beta_2 \text{ or } \beta_2 - \varepsilon]$ called watermark.

- Now we embed the resulting watermark into the Y components of I-frames by using locations that were previously saved. Namely, if the watermark value is β_1 or $\beta_1 - \varepsilon$, then we embed it into a location of the frame where its luminance is β_1, and if the watermark value is β_2 or $\beta_2 - \varepsilon$, we embed it into the location where its luminance is β_2. The mathematical relation in (11) illustrates the embedding equation.

$$I'(x,y)_y = \begin{cases} w(x)_{new} & \text{if } w(x)_{new} = \beta_1 \text{ or } \beta_1 - \varepsilon \\ & \quad \text{and } I(x,y)_y = \beta_1 \\ w(x)_{new} & \text{if } w(x)_{new} = \beta_2 \text{ or } \beta_2 - \varepsilon \\ & \quad \text{and } I(x,y)_y = \beta_2 \end{cases} \tag{11}$$

where $I(x,y)_y$ and $I'(x,y)_y$ are the original and modified luminance values, respectively. We may encounter a case which has not had enough locations and in fact the length of watermark is larger than numbers of locations that could be found in Y component of an I-frame.

In order to overcome this problem which in other words means to expand the capacity, we have to continue our search through the Y component until we find pixels whose luminance are near β_1 and β_2. During the watermark embedding "the seed of the tent map" parameters including a, β_1, and β_2 as well as the embedding locations are considered as keys so that without them extraction of logo is very hard.

Again, it should be mentioned that the reason for the selection of the I-frames is that their presence in a video sequence is necessary and the absence of even one frame reduces visual quality. One other advantage of embedding in these frames is that they can only be compressed to a low level and this helps reduce distortion due to tampering during embedding stage. Thus, this gives us a watermarking approach with high transparency result. It is worth mentioning also that compared to image watermarking, for a video sequence, we have a considerable number of I-frames and embedding capacity is relatively much higher than that of a still image.

4.3 Watermark Extraction

In order to obtain the logo image we need keys which were saved in the watermark embedding. The block diagram in Figure 2, illustrates how the logo image can be obtained. To extract the binary logo, we do the following steps:

(1) Separate the Y component of I-frames.
(2) Extract the luminance values from the saved locations (the receiver has the embedding positions coordinates as keys). In this step, we call these values as $g(x)$.
(3) Designate -1 and 1 to $g(x)$ values to obtain a bipolar sequence $p(x)$, in accordance with the following equation:

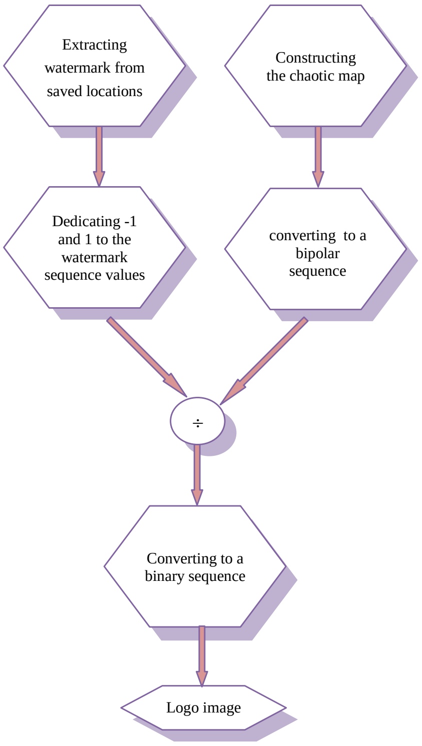
Extracting watermark from saved locations
Constructing the chaotic map
Dedicating -1 and 1 to the watermark sequence values
converting to a bipolar sequence
÷
Converting to a binary sequence
Logo image

Figure 2. Block diagram of obtaining the logo

$$p(x) = \begin{cases} -1 & \text{if } |g(x) - \beta_1| \leq |\beta_1 - \beta_2|/2 \\ 1 & \text{otherwise} \end{cases} \tag{12}$$

where $g(x)$ is the extracted luminance value and $p(x)$ is the bipolar sequence resulting from (12).

(4) By using (4), (5) and (6) the bipolar chaotic sequence is constructed. We now divide this sequence into $p(x)$. We call this resulting sequence as $w'(x)$. Then to obtain a binary sequence $q(x)$ we act as shown below:

$$q(x) = \begin{cases} 0 & \text{if } w'(x) = -1 \\ 1 & \text{if } w'(x) = 1 \end{cases} \tag{13}$$

Finally, to retrieve the logo image, we need to convert $q(x)$ to a two dimensional matrix.

5 Experimental Result

This section consists of two parts: the first part examines the simulation results when the proposed method is subjected to some usual attacks and the second part focuses on comparing these results with those obtained from existing watermarking algorithms. In our method, for each I-frame we generate a different watermark. This is done by just changing the seed of the chaotic map. Therefore, our method is robust to collusion attacks.

5.1 Simulation Results of Our Proposed Method

Table 1. Details of test videos and β_1, β_2 values

	Foreman	**Rush hour**	**Pedestrian**
Resolution	$352 * 288$	$720 * 576$	$720 * 576$
β_1	219	30	30
β_2	235	89	64

The logo is just a binary image (50 × 50) which is illustrated in Figure 3.d, and details of the video sequences utilized in the simulation, β_1, and β_2 values have been written in Table 1. The chaotic map we use is the tent map constructed by (4). Its seed is set by (5). We display robustness results for the first I-frame in Table 2. Distortion in an I-frame is measured by Peak Signal to Noise Ratio (PSNR):

$$PSNR = 10\log(\frac{255^2}{MSE})$$
$$MSE = \sum_{i=1}^{M}\sum_{j=1}^{N}|X(i,j) - X'(i,j)| \tag{14}$$

where $X(i,j)$ is the original signal and $X'(i,j)$ is the watermarked one.

We utilize Bit Error Rate (BER) to determine how the extracted logo is similar to an original logo. The following relation calculates the BER.

$$BER = \frac{B}{m \times n} \tag{15}$$

where B denotes the number of erroneously detected bits and $m \times n$ is the extracted binary watermark image dimensions. Parameter values which we use are: $x(0) = 0.01$, $a = 1.75$, $\varepsilon = 3$, and iteration of the tent map (n) is as same as the size of the logo i.e. 50 × 50. Note that values are decided according to explanations in embedding watermarking sub-section and as well as experiments.

In order to simulate the proposed method on the video sequences, the videos are first compressed using the MPEG-2 standard. Then their resistance versus different attacks is evaluated. Since there is a quantization stage in the MPEG-2 standard, this may cause a concern about the robustness of our method against compression. However, the results in Table 3, demonstrate that our method can extract the watermark signal completely i.e. with a zero BER.

The original I-frames and the watermarked I-frames are shown in Figure 3. It can be seen from Figure 3 that the watermarked frames are visually as crisp as the original ones. The PSNR and BER% results are shown in Table 2. It is clear from Table 2 that there should be no concern about JPEG compression. Also from this

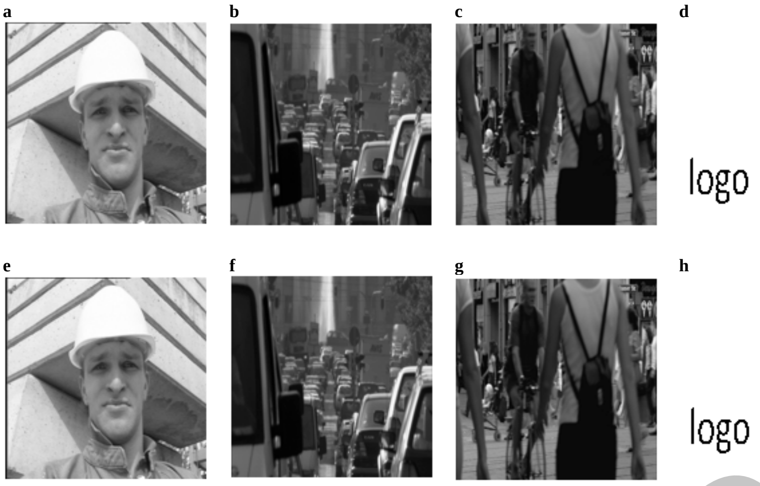

Figure 3. (a)–(c) are original frames. (d) is the original binary logo. (e)–(g) are the watermarked frame. (h) is the extracted logo.

Table 2. PSNR AND BER% results of our proposed method against some attacks

Attacks	Foreman		Rush hour		Pedestrian	
	PSNR	BER%	PSNR	BER%	PSNR	BER%
No attack	45.85	0.00	48.37	0.00	48.11	0.00
Salt & Pepper (0.01)	25.17	0.96	25.20	0.56	24.91	0.64
Median filter [3 3]	35.18	0.00	44.17	0.00	40.24	0.00
Median filter [5 5]	31.55	0.00	38.58	0.00	35.36	0.00
Average filter	31.01	0.24	42.36	0.00	38.75	0.00
JPEG (quality factor=80%)	37.76	0.00	44.80	0.00	43.72	0.00
JPEG (quality factor=60%)	35.52	0.36	42.61	0.00	41.44	0.00
JPEG (quality factor=40%)	34.08	0.72	40.78	0.00	39.54	0.00
Rotation 2°	22.28	0.00	27.78	1.10	26.73	0.60
Rotation 4°	18.92	0.00	24.88	2.70	23.78	2.30
Rotation 6°	17.05	0.00	23.22	3.80	22.11	3.00

Table 3. The PSNR and BER% values after applying the MPEG-2 standard on test videos

	Foreman	Rush hour	Pedestrian
PSNR	45.85	48.37	48.11
BER%	0.00	0.00	0.00

table, it is observed that our method has high resilience against filtering, rotation, and salt & pepper noise. We applied different types of filters to the watermarked frames, then we extracted the logo image. As the results in Table 2 shows the logo has been extracted without having any BER. Rotation is an attack that its aim is to move the pixels positions of frame. It is obvious from Table 2 that our watermarking method have a reasonable resistance against rotation. Figure 4. Also the results in Table 2 illustrates the same fact via using a bar diagram.

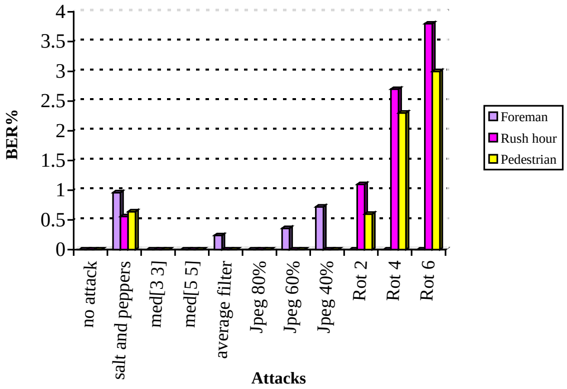

Figure 4. BER% of our proposed method against some attacks

Figure 5 illustrates the extracted logo from watermarked videos after applying some attacks. Note that in order to extract the logo from the rotated image, we

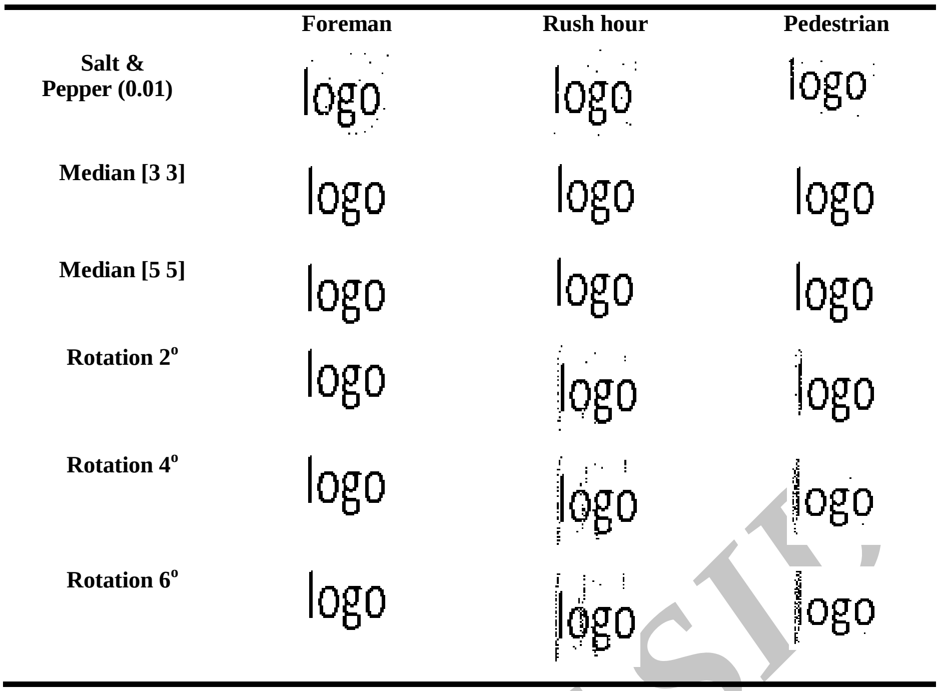

Figure 5. The extracted logos under different attacks.

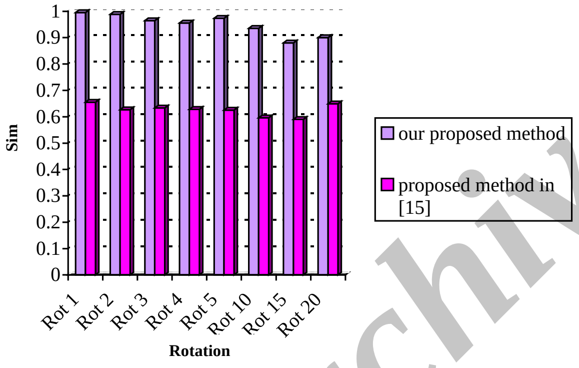

Figure 6. Comparison results between our method and method in [15] (the test video is flower-garden (sif))

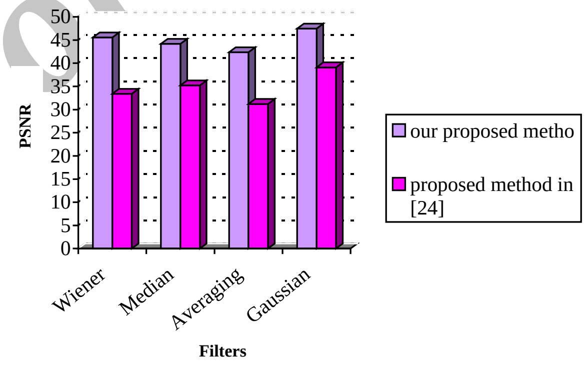

Figure 7. Comparison results between our method and method in [24], from PSNR viewpoint, under different types of filtering (BER under these filters is zero for both methods); (The test video is Rush Hour)

rotate the rotated image back and after each rotation-back, we calculate the BER between the extracted logo and the original logo to find the best extracted logo. It is significant that we embed 2500 bits in an I-frame (the number can be bigger) and in a video sequence there is more than one I-frame. Therefore, the capacity of our method is large.

5.2 Comparison Results

In this sub-section, we comprise resistance of our method with methods in [15] and [24]. The first comparison is between our method with method in [15]. In this comparison, the comparison parameter is considered as normalized correlation value and is calculated as follow:

$$sim = \frac{\nabla w' \times \nabla w^T}{\sqrt{(\nabla w' \times \nabla w'^T)\,(\nabla w \times \nabla w^T)}} \qquad (16)$$

where w' denotes the extracted watermark and w is the original watermark, exponent T stands for transpose and the ∇ is the gradient operation. The comparison results are presented in Figure 6. With respect to the Normalized Correlation values achieved by our method, it is obvious that compared to watermarking systems in [15], our method is more resistant to the rotation attack.

In another comparison, we comprise our method with the scheme in [24] from viewpoint of PSNR. Of course, it is noticeable to say that both methods in this paper and in [24] have zero BER against different types of filtering attacks. Figure 7 shows the comparison results. From this figure, it is clear that our method has more transparency.

6 Conclusion

A simple video watermarking algorithm with high resilience is proposed based on chaotic maps. The research focuses on spatial domain watermarking and shows that it exhibits potent defense against many unintended or malicious attacks (Table 2). To make the technique immune against collusion attacks, we embedded different watermarks in different frames. Experimental results show that our technique is effective. From the security perspective, given that watermarking based on tent map encryption was opted for, our method showed superior performance and good robustness, in comparison to other existing techniques. Since the method has evolved around spatial domain, it is independent of any compression standard and simplified computations are its hallmark. The comparison results indicate our results outperform the methods proposed in [15] and [24].

References

[1] Ester Yen and Li-Hsien Lin. Rubik's cube watermark technology for grayscale images. *Expert Systems with Applications*, 37(6):4033–4039, 2010.

[2] Tiegang Gao, Qiaolun Gu, and Sabu Emmanuel. A novel image authentication scheme based on hyper-chaotic cell neural network. *Chaos, Solitions and Fractals*, 42(1):548–553, 2009.

[3] Hazem Munawer Al-Otum and Nedal Abdul Samara. A robust blind color image watermarking based on wavelet-tree bit host difference selection. *Signal Processing*, 90(8):2498–2512, 2010.

[4] Maneli Noorkami and Russell M. Mersereau. A framework for robustbwatermarking of h.264/ avc-encoded video with controllable detection performance. *IEEE Transaction on Information Forensics and Security*, 2(1):14–23, 2007.

[5] Gwenael Doerr and Jean-Luc Dugelay. A guide tour of video watermarking. *Signal Processing: Image Communication*, 18(4):263 – 282, 2003.

[6] Karen Su, Deepa Kundur, and Dimitrios Hatzinakos. Statistical invisibility for collusion-resistant digital video watermarking. *IEEE Trans. Multimedia*, 7(1):43–51, 2005.

[7] Muhammad Khurram Khan, Jiashu Zhang, and Lei Tian. Chaotic secure content-based hidden transmission of biometric templates. *Chaos, Solitions and Fractals*, 32(5):1749–1759, 2007.

[8] Narendra Singh and Aloka Sinha. Digital image watermarking using gyrator transform and chaotic maps. *International Journal for Light and Electron Optics (Optik)*, 121(15):1427–1437, 2010.

[9] Jiashu Zhang, Lei Tian, and Heng-Ming Tai. A new watermarking method based on chaotic maps. In *IEEE International Conference on Multimedia and Expo (ICME)*, 2004.

[10] S. Behnia, M. Teshnelab, and Ayubi P. Multiple-watermarking schem based on improved chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 15(9):24692478, 2010.

[11] Xianyong Wu and Zhi-Hong Guan. A novel digital watermark algorithm based on chaotic maps. *Physics Letters A*, 365(5-6):403–406, 2007.

[12] Rongrong Ni, Qiuqi Ruan, and Yao Zhao. Pinpoint authentication watermarking based on a chaotic system. *Forensic Science International*, 179(1):54–62, 2008.

[13] Siyue Chen and Henry Leung. Chaotic watermarking for video authentication in surveillanc applications. *IEEE Transactions on Circuits and Systems for Video Technology*, 18(5):704–709, 2008.

[14] Somayyeh Mohammadi, Siamak Talebi, and Ahmad Hakimi. A secure and robust video watermarking based on chaotic maps. In *8th Iranian Security Community Conference*, 2011.

[15] Yan Liu and Jiying Zhao. A new video watermarking algorithm based on 1D DFT and Radon transform. *Signal Processing*, 90(2):626–639, 2010.

[16] Radu O. Preda and Dragos N. Vizireanu. A robust digital watermarking schem for video copyright protection in the wavelet domain. *Measurement*, 43(10):17201726, 2010.

[17] Dooseop Chio, Hoseok Do, and Taejeong Kim. A blind Mpeg-2 video watermarking robust to camcorder recording. *Signal Processing*, 90(4): 13271332, 2010.

[18] Alper Koz and A. Aydin Alatan. Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system. *IEEE Transactions on Circuits and Systems for Video Technology*, 18(3):326 – 337, 2008.

[19] Bijan G. Mobasseri, Michael J. Sieffert, and Richard J. Simard. Content authentication and tamper detection in digital video. In *Proceeding of IEEE International Conference on Image Processing*, volume 1, pages 458 – 461, 2000.

[20] Dengpan Ye, Changfu Zou, and Zhiquan Wang. A new adaptive watermarking for real-time MPEG videos. *Applied Mathematics and Computation*, 185(2):907–918, 2007.

[21] Jing Zhang, Anthony T. S. Ho, Gang Qiu, and Pina Marziliano. Robust video watermarking of H.64/AVC. *IEEE Transactions on Circuits and*

System-II: Express Briefs, 54(2):205–209, 2007.

[22] Hae-Yeoun Lee, Hyungshin Kim, and Heung-Kyu Lee. Robust image watermarking using local invaraint features. *Optical Engineering*, 45(3): 37001–37002, 2006.

[23] Hefei Ling, Liyun Wang, Fuhao Zou, Zhengding Lu, and Ping Li. Robust video watermarking based on affine invariant regions in the compressed domain. *Signal Processing*, 91(8):1863–1875, 2011.

[24] Maneli Noorkami and Russell M. Mersereau. Digital video watermarking in p-frames with controlled video bit-rate increase. *IEEE Transactions on Information Forensics and Security*, 3 (3):441 – 455, 2008.

[25] Guang-yong Gao and Guo-ping Jiang. 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, 2011.

[26] Yu-feng Hu and Shan-an Zhu. Zero-watermark algorithm based on PCA and chaotic scrambling. *Journal of Zhejiang University: Engineering Science*, 42(4):593–597, 2008.

[27] Sanjay Rawat and Balasubramanian Raman. A chaotic system based fragile watermarking scheme for image tamper detection. *International Journal of Electronics and Communications (AEU)*, 65(10):840847, 2011.

[28] Mohammed Ghanbari. *Standard codecs: Image compression to advanced video coding (IET telecommunications series)*. The Institution of Engineering and Technology, 2003.

[29] Kathleen T. Alligood, Tim D. Sauer, and James A. Yorke. *Chaos: an introduction to dynamical systems*. Springer, 2001.

Somayyeh Mohammadi received the BSc and MSc degrees in electrical and communication engineering from Shahid Bahonar University of Kerman, Kerman, Iran, in 2008 and 2011, respectively. Her current research interests are in image and video processing field, especially in design of image and video watermarking systems.

Ahmad Hakimi received the BSc degree in electrical engineering from Technical College of Shahid Bahonar University of Kerman, Kerman, Iran, in 1986. Using the scholarship which was granted by the Ministry of Higher Education of Iran and Istanbul Technical University (ITU) in 1987, he studied for the degree of MSc and PhD in the faculty of electrical and electronic at the ITU. He received the MSc and PhD degrees from ITU in 1996 and 1995 in the field of high-frequency electronics. His research interests include the design and analysis of nonlinear RF circuits, numerical analysis and advanced engineering mathematics, analog filter. He is currently a member of the faculty at the Design and Industrial Research Center, Kerman, Iran, and Department of Electrical Engineering, Shahid Bahonar University of Kerman, Kerman, Iran.