Two Novel Chaos-Based Algorithms for Image and Video Watermarking

S. Mohammadi*, S. Talebi** and A. Hakimi*

Abstract: In this paper we introduce two innovative image and video watermarking algorithms. The paper's main emphasis is on the use of chaotic maps to boost the algorithms' security and resistance against attacks. By encrypting the watermark information in a one dimensional chaotic map, we make the extraction of watermark for potential attackers very hard. In another approach, we select embedding positions by a two dimensional chaotic map which enables us to satisfactorily distribute watermark information throughout the host signal. This prevents concentration of watermark data in a corner of the host signal which effectively saves it from being a target for attacks that include cropping of the signal. The simulation results demonstrate that the proposed schemes are quite resistant to many kinds of attacks which commonly threaten watermarking algorithms.

Keywords: Chaotic Maps, Resistance, Security, Watermarking, Wavelet Transform.

1 Introduction

In recent decades, the necessity of protecting multimedia data has led to the development of a variety of watermarking techniques [1-4]. One major concern with most of these techniques is their security. The quest for high security in watermarking methods is incessantly driving the desire for more complex approaches [5]. However, schemes which enjoy enhanced security features are complicated, very costly and require a lengthy time for embedding and extracting watermark information which therefore makes them cumbersome for any practical application. In order to overcome these challenges and devise a dependable platform, new methods based on chaotic maps has been put forward [6-8]. Up to now, though, only a handful of watermarking techniques based on chaotic maps have emerged [7-12], in which the majority concentrate on image watermarking [7-11] with only a few studying the algorithm for its video counterpart [12].

In general, transparency, resistance, security, an capacity are four main parameters that define efficiency of a watermarking technique [11]. However in the case of video, simplicity of a given method, is also a vital deciding factor since it means less computations is involved and therefore increased speed can be expected. The significance of this criterion becomes rather more obvious when a live video is broadcasting. Let's now see how we can overcome the challenges and develop a system that requires minimum computation and at the same time offers maximum resistance and security.

In general, watermarking methods are divided into spatial domain and transform domain [13-15]. In classifying watermarking techniques, video compression standard is also, of course, a consideration and therefore has to be further categorized as either compressed video or uncompressed video watermarking [16-20]. Now, given that simplicity and high speed are hallmarks of spatial domain watermarking algorithms, it is unfortunate that these processes on the whole suffer from the drawback of weak resistance against attacks which is the result of tampering with least significant bits (LSB) of the images or video frames [9].

Methods which, in order to embed watermark data, transfer host signal to the transform domain do so to guarantee high resistance. However, on the whole working in the transform domain inevitably leads to increased computational complexities and a consequent loss of speed.

Any raw video signal consists of several frames which increases the volume of video clip and therefore needs to be compressed. As was mentioned earlier, in video watermarking, embedding can take place either

Iranian Journal of Electrical & Electronic Engineering, 2012
Paper first received 31 Dec. 2011 and in revised form 08 May 2012.

*,** The Authors are with the Department of Electrical Engineering Shahid Bahonar University of Kerman, Kerman, Iran.
** The Author is also with the Advanced Communications Research Institute at Sharif University of Technology, Tehran, Iran
E-mails: mohammadi_0313@yahoo.com, siamak.talebi@uk.ac.ir, hakimi@uk.ac.ir.

before or after the compression stage. With the uncompressed option, compression itself becomes an attack since current techniques include a quantization step which results in the loss of information. In watermarking systems, this process is interpreted as an attack and therefore for such an application one must ensure that watermarking algorithm has sufficient strength to withstand compression. On the other hand, when opting for watermarking after video signal is compressed, one has to be watchful of unwanted bit rate increases.

In [8], the proposed method uses chaotic maps in the form of constructed chaotic random phase masks (CRPM) that are multiplied in a logo image. Let us explore the approach in more details; logo image is first multiplied by a CRPM consisting of two one dimensional (1-D) chaotic maps and then in order to boost system's security, the resulting image is transferred by Fractional Fourier transform (FRFT) where in this transform domain another CRPM, which has been constructed from two 2-D chaotic maps, is multiplied by logo image and again FRFT transform is applied. The authors of this method argue that the reason for such a watermark embedding in chaotic maps and the application of FRFT is to increase the number of keys, which in other words mean to boost watermarking system's security. In this technique, after the completion of the process, the logo image is added to the host image.

The proposed method in [9] considers a 128×128 pixel binary image as watermark information. Here, for embedding watermark bits, they have come up with the idea of embedding in the least significant bits (i.e. bit numbers 3, 4, 5, and 6) of the host image and in order to determine the pixel bit of host image which is the position for embedding watermark bits, they have used a 1-D chaotic map. The authors also take advantage of another chaotic map to encrypt the embedding positions of the host image. It should be mentioned that in this scheme the host image is in RGB color in which one logo image is considered for each of the three components.

Now, a review of the method put forward in [2] tells us that in this case researchers first divide the frames of a video clip into equal sets. They then apply a 1-D discrete Fourier transform (DFT) to these sets and finally select frames with highest coefficients. Subsequently by subjecting frames with the highest temporal frequencies to Radon transform [21], watermark is embedded. In this scheme, authors deal with RGB color video clip and embedding process takes place on the blue channel of the selected frames. At this point, watermark information is generated by a pseudo random generator, which is a spread spectrum consisting of positive values. In their implementation, they generate 32 random numbers. Then, they spread the generated random numbers into a watermark pattern w by zero-padding in between the generated random numbers. In this method the length of w equals the horizontal width of target video frame.

An examination of the watermarking system in [4] reveals that wavelet transform is applied in two levels to luminous component of the frames in a video clip and then embedding takes place in wavelet coefficients. In this study, the watermark bits are embedded in the host signal by making wavelet coefficients odd and even.

In this paper, we exploit some of the main properties of chaotic maps in order to develop image and video watermarking algorithms with high resistance and security features. We also unveil a spatial domain algorithm that not only enhances the performance of the simple algorithm, but also overcomes its weak resistance by the particular way it embeds watermark information in the host signal. The innovative technique which encompasses both image and video signals displays impressive resistance against attacks as has been verified by simulation results. This research work is also going to tackle the challenge posed by video watermarking by introducing a system that is based on wavelet transform and exhibits potent resistance at low computational complexity.

The rest of this paper is organized as follows: In section 2, chaotic maps are explained which is followed by a disclosure in section 3 of the proposed techniques for image and video watermarking based on chaotic maps. Two methods are presented in depth one for video watermarking and the other for image watermarking. The latter's potential is also further examined for video applications. Simulation results and comparisons with other approaches are given in section 4. In the concluding section, the paper highlights the main achievement of the proposed techniques and some of their striking features.

2 Chaotic Maps

Chaos is defined by a Lyapunov exponent greater than zero. Lyapunov number $L(x_1)$ defined as [22]:

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

where n and $f(x)$ are the map and iteration number, respectively. Also the Lyapunov exponent $h(x_1)$ can be defined as:

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

where n and $f(x)$ are the map and iteration number, respectively . Some of the exciting properties of chaotic maps and the motive behind their applications in watermarking techniques include:

- Sensitivity to initial conditions
- Unpredictability
- Non-periodicity

- No correlation between numbers generated by two chaotic maps that have two different seeds.

The three chaotic maps utilized in this study are as follows:

1. A 1-D chaotic map called Tent map, constructed from the following equation, [8]:

$$\begin{aligned} x_{n+1} &= a x_n & \text{for } 0 \le x \le 0.5 \\ x_{n+1} &= a(1-x_n) & \text{for } 0.5 \le x \le 1 \end{aligned} \qquad (3)$$

In this equation a denotes chaotic parameter and $0 < a \le 2$. also, n is the iteration number.

2. A 1-D chaotic map called Logistic map which can be expressed by the following relationship [8]:

$$x_{n+1} = \rho x_n (1 - x_n), \qquad (4)$$

where $0 < \rho < 4$.

3. A 2-D chaotic map called Kaplan-Yorke map [8] which is defined as:

$$\begin{aligned} x_{n+1} &= a x_n \bmod 1 \\ y_{n+1} &= b y_n + \cos(4\pi x_n) \end{aligned} \qquad (5)$$

where a and b are chaotic parameters so that $0 \le a \le 2$ and $0 \le b \le 1$.

By a suitable selection of chaotic parameters namely a, b, and ρ these maps will display chaotic behavior.

Due to sensitivity to initial conditions, seeds can be regarded as keys. On the other hand, chaotic parameters themselves can also be counted as other keys, where their presence will increase security of the watermarking technique. Hence, the greater the dimensions of a chaotic map in a watermarking system, the bigger the corresponding number of seeds and chaotic parameters. This results in an increase in the number of keys which therefore gives rise to better security for the system.

3 Proposed Methods

In this section two watermarking algorithms are proposed. The first algorithm focuses on color and gray images which will be extended to include video signals. The second algorithm is exclusively devoted to video watermarking.

3.1 Image Watermarking Algorithm Based on Chaotic Maps

We begin our approach by first multiplying a binary logo image by a Logistic map (4), whereby making extraction of watermark for any attacker difficult. This action effectively encrypts the logo in the Logistic map. Before multiplying, of course, the Logistic map and logo are converted to bi-polar sequences consisting of 1 and -1 as follows:

$$l(x) = 2(g(x)) - 1 \qquad (6)$$

$$x_{n-bipolar} = 2(round(x_n)) - 1, \qquad (7)$$

where $g(x)$ denotes a binary logo that has been converted to a vector, $l(x)$ is the resulted bi-polar vector and x_n is a sequence constructed from Eq. (4). And $x_{n-bipolar}$ is a bi-polar sequence. Note that the chaotic map's length is equal to the number of logo bits and the seed is a number between zero and one. We call the sequence resulting from multiplication, as watermark, which includes {-1, 1} and then, we embed the watermark in the host signal. This is how the embedding process is carried out:

To begin, we search the entire host signal to find two pixels whose intensities have more repetition over the host signal. We call these values β_1 and β_2 where β_1 must be less than β_2. In order to have more resilience to attacks such as image processing, the magnitude of distance between β_1 and β_2 should be reasonable so that it can be obtained by experiment. Next, we store positions of pixels with β_1 and β_2 intensities and then change the watermark bits as follows:

$$\begin{cases} -1 \to \beta_1 - \varepsilon \\ \ \ 1 \to \beta_2 - \varepsilon \end{cases} \qquad (8)$$

where ε is an integer greater than 1 which, of course, for maximum transparency of the watermarked image must not be very big and can best be found by some trial and error. Also, for still more transparency, ε in (8) can be considered only for the case when:

$$\begin{cases} -1 \to \beta_1 - \varepsilon \\ \ \ 1 \to \beta_2 \end{cases} \qquad (9)$$

or

$$\begin{cases} -1 \to \beta_1 \\ \ \ 1 \to \beta_2 - \varepsilon \end{cases} \qquad (10)$$

Having made these changes, watermark information of the form $\{\beta_1 \ or \ \beta_1 - \varepsilon, \beta_2 \ or \ \beta_2\}$ is now embedded in host image positions whose addresses where previously stored and the search should continue for as long as it takes for all logo bits to be embedded. Since lack of sufficient number of locations (under this condition) to embed all watermark bits is also a possibility, the problem can be solved by accommodating the remaining bits in locations whose intensities are nearest to β_1 and β_2. It should be noted that embedding locations, β_1, β_2, and ε are regarded as seeds and the chaotic parameter as keys without which it would be impossible to extract watermark information. Fig. 1 shows the required steps to obtain a watermarked image.

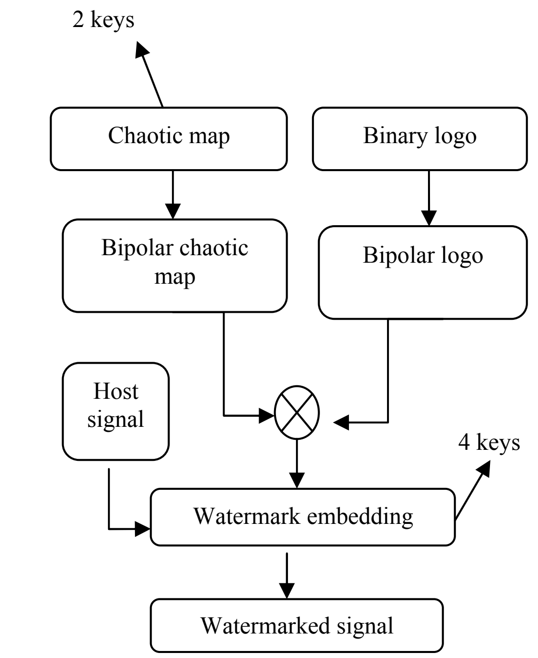


Fig. 1 Block diagram of watermark embedding.

The extraction process is exactly the reverse of embedding process which can be performed if the receiver has information about the type of chaotic map. Being deployed, its seed, β_1, β_2, ε, the chaotic parameter, and embedding positions. Now, having extracted watermark from those known locations and in order to obtain the binary logo image.

These values are first converted to 1 and -1 in accordance with the following expression:

$$p(x)=\begin{cases}-1 & if\left|w(x)-\beta_1\right|\prec\left|\beta_1-\beta_2\right|/2\\ 1 & other\ else\end{cases} \qquad (11)$$

where $w(x)$ denotes the extracted watermark. Next, by dividing $p(x)$ by Eq. (7) and converting resulting values to a 0 and 1 sequence of the form:

$$q(x)=\begin{cases}0 & p(x)=-1\\ 1 & p(x)=1\end{cases} \qquad (12)$$

Finally, by converting the $q(x)$ vector to a 2-D matrix, we obtain in the binary logo. Fig. 2 outlines the steps to extract logo image.

3.2 Video Watermarking Algorithm Based on Chaotic Maps in the Spatial Domain

The algorithm that we are going to unveil here is derived from the previous sub-section but care should be taken that in order to prevent the video watermarking algorithm from being vulnerable to collusion attacks, for each I frame, separate watermark is set aside. The reason for this is that a watermark system will be vulnerable to collusion attacks when the same watermark is embedded in different frames or when different watermarks are embedded in frames that are very similar to one another. The vulnerability arises because under this setting, by frame averaging, a potential attacker can easily estimate the watermark pattern and either extract or destroy it. In order to generate separate watermark patterns. We only have to change the seed of the chaotic map each time we multiply it by the watermark. This is because chaotic maps are sensitive to initial conditions, as we mentioned in section 1, we have selected luminance component (Y) of I frames of video clips for embedding watermark bits and in order not to exceed side information transmission, the seed is defined as follows:

$$x(0)=\frac{frame\ index}{100}. \qquad (13)$$

We have developed this algorithm for video clips that compressed with MPEG-2 compression standard. However, since embedding process can be carried out before compression the approach can find applications with many other standards. The point to bear in mind is that here compression should be viewed as an attack. None the less, as simulation results in section 4 shows there needs to be no worries about the algorithm's resistance to neutralize compression attacks too.

It is important to note that the reason for the selection of the I-frames is the necessity for their presence in a video sequence. Since these frames are compressed to a low level, their inclusion helps reduce distortion due to tampering during the embedding stage. Thus, this results in a highly transparent watermarking approach. It is worth mentioning also that compared against image watermarking, in a video sequence we have a considerable number of I-frames and embedding capacity is relatively much higher than that of a still image.

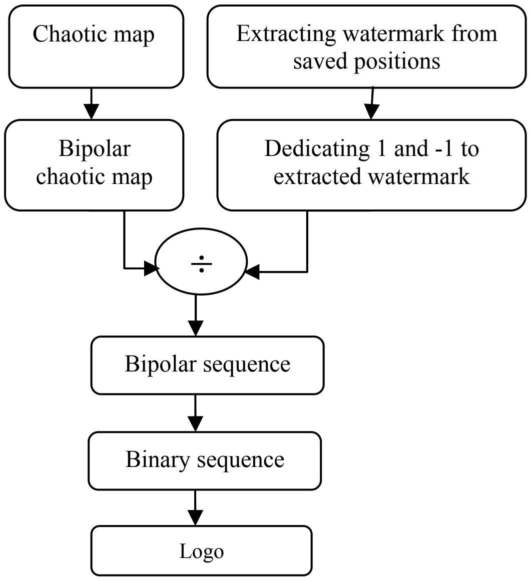

Chaotic map
Extracting watermark from saved positions
Bipolar chaotic map
Dedicating 1 and -1 to extracted watermark
÷
Bipolar sequence
Binary sequence
Logo

Fig. 2 Block diagram of watermark extraction.

3.3 Video Watermarking Algorithm Based on Chaotic Maps and Wavelet Transform

Let us break the proposed algorithm into three consecutive steps and explain each one in turn, as follows:

- Watermark generation
- Watermark embedding
- Watermark extraction

3.3.1 Watermark Generation

Watermark information can take the form of an image (logo) or of a binary sequence. In order to generate watermark, the logo image or a binary sequence which converted into a bi-polar sequence is multiplied by the Tent map that has been constructed by Eq. (3) and converted into a bi-polar sequence by Eq. (7). We call the resulting sequence a watermark. As mentioned above, in order to generate different watermarks, it is only necessary to change the seed of chaotic map. In order to avoid sending the receiver excessive information, we define the seed Eq. (3) in the form of Eq. (13). It is clearly seen that by changing frame index, we will have different chaotic map seeds and therefore many number of watermarks corresponding to each I frame.

3.3.2 Watermark Embedding

We have selected luminance component (Y) of video clip's I frames for watermark embedding. Embedding takes place in the wavelet domain and before compression stage (i.e. in the uncompressed domain). In order to increase the method's resistance, wavelet transform is applied to the host video signal in three levels and HL3 sub-band is set aside for our embedding purposes, (Fig. 3). This sub-band was selected for watermark embedding in order both to enjoy the resistance advantage in this level of wavelet decomposition and to maintain the quality of the video signal. Of course, in order to ensure that the choice for sub-band was suitable, some trial and error was undertaken. The coordinates of HL3 sub-band coefficients which will be modified in order to embed watermark bits, are selected by using the chaotic map constructed by Eq. (5). In order to relate the values generated by this chaotic map to the HL3 sub-band coefficients coordinates we modify the values derived from Eq. (5), as follows:

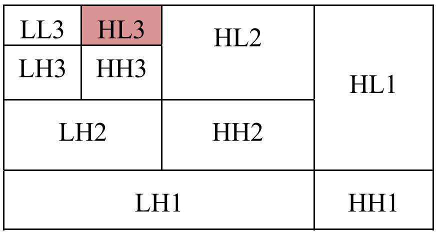


Fig. 3 The sub-band selected for embedding region.

$$\begin{aligned} x_n &= round\left(x_n\right) \\ y_n &= \mathrm{mod}\left(round\left(\left|y_n\right|\right),2\right) \end{aligned} \quad (14)$$

Now, we have two binary sequences consisting of {0,1} so we assign one sequence for rows numbers addressing and the other for columns numbers addressing. The way we do this is to break each one of the binary sequences Eq. (14) into sets of μ bits and then convert each one of these binary sets into its equivalent decimal number where the decimal numbers relate to the intended embedding locations columns and rows numbers. Care should be taken with the choice of μ so that the generated decimal number does not exceed maximum amount of HL3 rows and columns numbers. In order to better understand the technique for selecting HL3 sub-band coefficients, we have explained the steps through an example in the at the end of this sub-section; still, the following statements are also noteworthy.

We may come across a case where generated decimal number is zero. Since we already know that minimum column and row number is 1, this hitch can be resolved by adding one unit to all generated numbers during the last step.

It is also always possible that after rounding and converting binary numbers to equivalent decimal numbers we may end up with some repeat numbers. Again, given that it is not possible to embed more than one bit in a position, from the start we make length of the chaotic map (constructed by Eq. (5)) at least twice bigger than the number of watermark bits. This action ensures that there is still sufficient numbers available for embedding even after eliminating repeat numbers.

The last point of concern is that in order to be able to easily separate the μ sets of binary sequences, we need to ensure that the sequence length from Eq. (5) is always a multiple of μ.

After selecting coefficients from HL3 sub-band that must be modified during watermarking process, the next thing to do is to embed bi-polar watermarks consisting of {-1, 1} which were generated in previous sub-section the selected HL3 sub-band coefficients are changed in such a way that:

$$HL3\left(i,j\right)=\begin{cases}\beta w\left(x\right) & if\ w\left(x\right)=1\\ w\left(x\right) & if\ w\left(x\right)=-1\end{cases} \quad (15)$$

where $w\left(x\right)$ denotes watermark sequence, β is the watermarking factor, $HL3$ is the sub-band of the third wavelet decomposition level of an I frame, and $\left(i,j\right)$ is coordinate of the coefficient which we will see later in this sub-section how it is obtained. The choice of β value depends on to what extend quality of watermarked frame should be preserved as well as on the measure of resistance to attacks such as image processing. After several trial and errors, we found 25 is an optimum value for β. It should be mentioned that seeds and chaotic parameters Eq. (3) and Eq. (5) are both considered as keys and their transmission is necessary for the receiver.

HL3 sub-band coefficients selection:

Let's now explain how selection of the embedding positions is made by looking at an exmple:

Suppose that we have built the chaotic map defined by (5) and eighteen of the resulting numbers from this sequence is as follows:

x can have these values:

{0.5654, 0.341, 0.9180, 0.298, 0.365, 0.49, 0.2, 0.5409, 0.6791, 0.8901, 0.765, 0.91, 0.0281, 0.8756, 0.1019, 0.329, 0.8729, 0.9916}.

and *y*:

{1.905, 0.4532, 0.9867, 0.6, 0.949, 0.92, 0.991, 3.0987, 4.098, 0.0897, 0.4376, 1.098, 2.087, 2.0939, 2.8319, 1.8345, 0.342, 1.0201}.

Now, from (14), *x* can have these values:

{1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1}.

and y:

{0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1}.

If we consider this algorithm for a video clip with a 720×576 resolution, then the size of HL3 sub-band will be equal to 90×72. Now μ is selected such that when we have converted x_n and y_n binary sequences to equivalent μ sets of decimal numbers, for rows, no number higher than 90 and, for columns, no number higher than 72 is generated. In this example the best choice for μ is 6. Therefore from x_n and y_n binary sequence we separate digits in groups of 6 and convert them to an equivalent decimal numbers.

Thus we have for x_n:

{40, 15, 19}.

and for y_n:

{11, 49, 9}.

Finally, generated numbers resulting from x_n is assigned to rows numbers and generated numbers by y_n is assigned to columns numbers of HL3 sub-band coefficients coordinates that we are going to modify them in watermark embedding step. In this example, coefficients with these coordinates (40,11), (15,49), and (19,9) are selected as embedding positions.

3.3.3 Watermark Extraction

The extraction process is exactly the reverse of embedding process which requires construction of chaotic maps Eq. (3) and Eq. (5) by using keys that were deployed during embedding step. As in embedding step, first, wavelet transform is applied over three levels to luminance component of I frames. Then, to extract the watermark from coefficients of HL3 sub-band, we find the modified coefficients coordinates by using Eq. (5), Eq. (14), and the explanation in previous sub-section, thus we have:

$$w'(x) = \begin{cases} 1 & if\, HL3(i,j) \geq round\left(\dfrac{\beta}{2} - 3\right) \\ -1 & otherelse \end{cases} \qquad (16)$$

where (*i,j*) is a HL3 sub-band coefficient coordinate which was tampered with during embedding step, β is the watermarking factor, and $w'(x)$ is the extracted watermark. In order to obtain the binary sequence it is only necessary to divide $w'(x)$ by Eq. (3) which, as a result of applying Eq. (7), has become bi-polar and then restore the resulting bi-polar vector to a binary sequence.

4 Simulation Results

In this section, we present simulation results of our watermarking algorithms which have been subjected to a variety of potential attacks and also compare their features vis-à-vis other proposed methods concerning video and image signals.

4.1 Resistance Evaluation

4.1.1 Image Watermarking Results

We selected a 64×64 pixel binary image as the watermark information and a 512×512 pixel gray image (Stream and bridge image) to represent our host image. The chaotic map was constructed using Eqs. (4) and (7), taking $x_0 = 0.159$ as seed with ρ =3.84. Also, by way of trial and error as well as with reference to the explanation in sub-section 3.1 from section 3, we set values for β_1, β_2, and ε as 57, 85, and 4 respectively and applied Eq. (9) for modifying sequence numbers 1 and -1. Fig. 4 shows the original host image and the original binary logo image. In Fig. 5 the watermarked host image and the extracted binary logo image are displayed. The algorithm has been tested to determine the efficiency under common attacks such as JPEG compression, salt and pepper noise, rotation and filtering.

Table 1, illustrates the peak signal-to-noise ratio (PSNR) results between the original host image and the watermarked image as well as bit error rate (BER) percentage for the extracted watermark which is calculated as follows:

$$BER = \frac{B}{m \times n} \times 100, \qquad (17)$$

where *B* denotes the number of erroneously detected bits and $m \times n$ is total watermark bits. The resistance against JPEG compression attack for various qualities (QF) is assessed and as can be seen the system is quite resistant even with low QFs. It can also be observed from Table 1, that with increases in the salt and pepper noise density, although PSNR value reduces, we can still extract watermark completely. Therefore, from this table, it can be deduced that the proposed method is also very robust when faced with filtering attacks. Fig. 6, displays the extracted watermarks after being subjected to some common attacks.

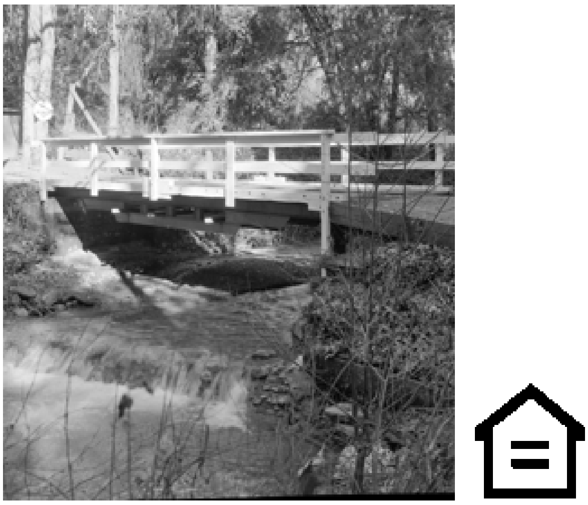


Fig. 4 The original host image and the original binary logo image (from left to right).

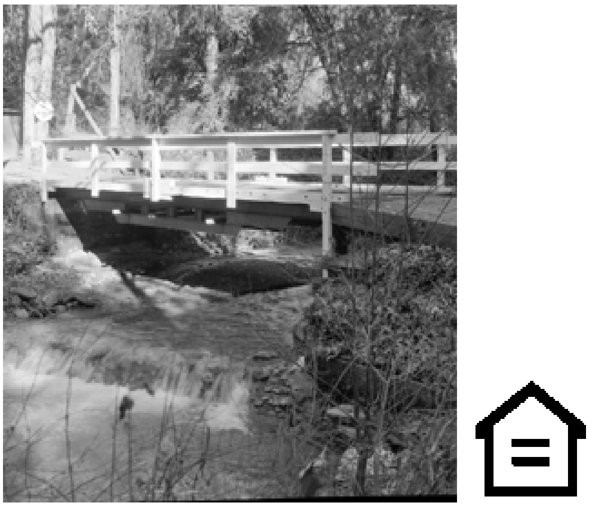


Fig. 5 The watermarked image and the extracted logo (from left to right).

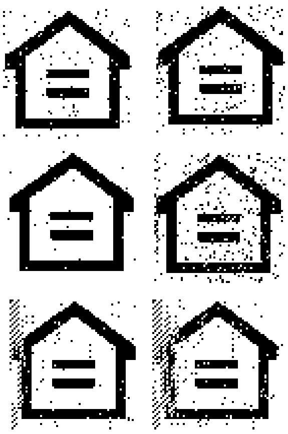


Fig. 6 Extracted logos under different attacks: JPEG (QF=60%), JPEG (QF=40%), Salt & Pepper noise (0.01), Median Filter [3 3], Rotation 3°, Rotation 7°, (from up to down and left to right respectively).

Table 1 Results of our proposed image watermarking.

Attacks	PSNR	BER%
No-attack	56.61	0.00
JPEG (QF-60%)	30.30	2.40
JPEG (QF-40%)	28.85	4.00
Rotation 3°	22.91	4.00
Rotation 7°	19.55	7.70
Salt & Pepper (0.01)	25.27	0.60
Median Filter [3 3]	26.72	6.80

4.1.2 Simulation Results of our Proposed Video Watermarking Algorithm in the Spatial Domain

Now we examine the resistance offered by the algorithm introduced in sub-section 3.2 from section 3.

Let's choose a binary logo image of size 64×64 as our watermark information and the Pedestrian video clip, (99 frames and 720×576 resolutions). With the help of Eqs. (3), (7), and (13), we construct the Tent map. Table 2, shows the resistance that can be expected when the algorithm is subjected to a number of common attacks. In this simulation the parameters are set as follows: x_0=0.01, a=1.75, β_1=30, β_2=64, ε=3, and the iteration number of Tent map is as many as logo bits. Figs. 7 and 8, depict the original and watermarked frame as well as the original and extracted logo respectively. In order to prove the proposed method's ability to embed different logos a more complex logo, e.g. that of our University logo was examined.

As was mentioned before, since our watermarking method is performed on uncompressed video we had to ensure that it could withstand compression attacks. By looking at Table 2 we see the result clearly provides the necessary assurance and also that it confirms the proposed approach's capabilities to counter attacks that emanate from noising and filtering as well as rotation. Fig. 9 displays extracted logo images after facing a number of common attacks.

4.1.3 Simulation Results of our Proposed Video Watermarking Method in the Wavelet Domain

In this sub-section, we assess the functionality of the proposed video watermarking algorithm based on wavelet transform by considering on a 50 bits long binary sequence. The video clip under investigation is the Pedestrian video clip (99 frames and 720×576 resolutions). By utilizing Eqs. (3), (7), and (13), we have

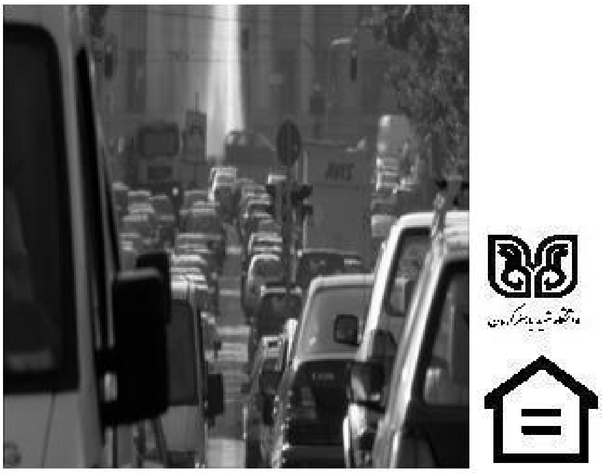


Fig. 7 The original frame and two original binary logos (from left to right).

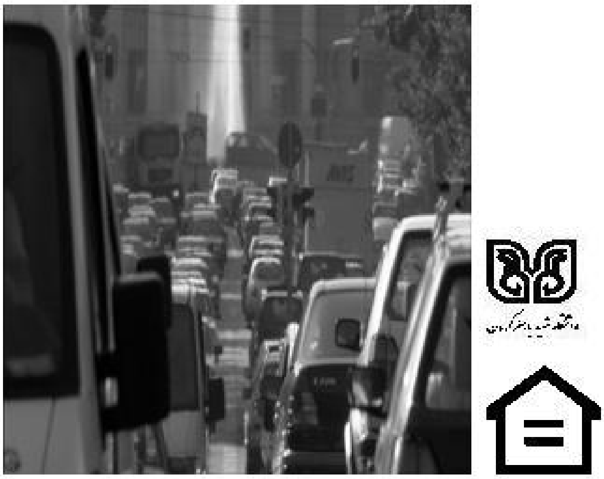


Fig. 8 The watermarked frame and two extracted logos (from left to right).

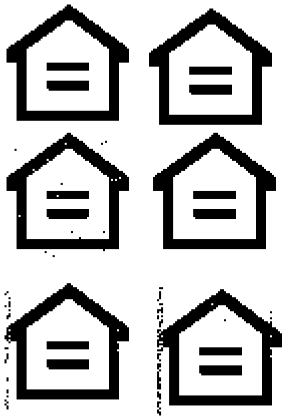


Fig. 9 Extracted logos under different attacks: JPEG (QF=60%), JPEG (QF=40%), Salt & Pepper noise (0.01), Median Filter [3 3], Rotation 3^{o}, Rotation 7^{o}, (from up to down and left to right).

constructed the Tent map. As we have already stated the result relating to the first I frame, therefore according to Eq. (13) the seed of Eq. (3) is 0.01 and the chaotic parameter of Eq. (3) is 1.75. Also, based on the explanation under the watermark embedding sub-section, embedding positions have been selected by using Eqs. (5) and (14), seeds are x_0=0.19, y_0=0.6 and chaotic parameters are a= 1.87 and b =0.9. In Figs. 10 and 11, the original host frame and watermarked frame are displayed respectively. From these figures, we can see very well that the quality of the watermarked frame has been preserved and that it very much resembles to the original host frame.

Also, Table 2, reflects the level of resistance we can expect from the proposed method when it is subjected to some common attacks. In this same table, both the quality level of the watermarked frame versus PSNR as well as the resulting error in extracting watermark versus BER have been compared. The results indicate that the proposed method enjoys a satisfactory level of resistance against JPEG compression attacks. Another advantage of this algorithm which is also reflected in Table 2 is that it provides high resistance when exposed to rotation attacks.

4.2 Comparison Results

Now, in this sub-section let us examine the results shown in Table 3 which compares our proposed image watermarking method introduced in sub-section 3.1 from section 3, versus the proposed method in [9] both from the perspectives of PSNR between original host image and watermarked image as well as resulted BER in extracting the watermark. In this case, host image is a RGB Lena image (512×512 sizes) and watermark information consists of a 128×128 pixel binary image. Additionally, for each of the three color components a watermark image has been considered. It is obvious that our method is more resistant compared to [9].

In another comparison, we comprise our algorithm with a new chaos watermarking [23] and then made BER evaluations. As the charts in Fig. 12, displays far superior resistance and better detection powers against attacks in comparison with that proposed in [23].

By referring to Table 4, we take a look at the results of our video watermarking methods introduced in sub-section 3.2 and 3.3 from section 3 to see how they compare with the algorithm put forward in [2] which was outlined in the introduction section. For the purpose of comparison, the test video clip is Foreman (352×288 resolutions). Since in [2], measurement of resemblance between extracted watermark and original watermark is based on the criterion calculated by (18) below, we also choose our criterion based on this formula:

$$sim = \frac{\nabla w' \times \nabla w^{T}}{\sqrt{\left(\nabla w' \times \nabla w'^{T}\right)\left(\nabla w \times \nabla w^{T}\right)}} \qquad (18)$$

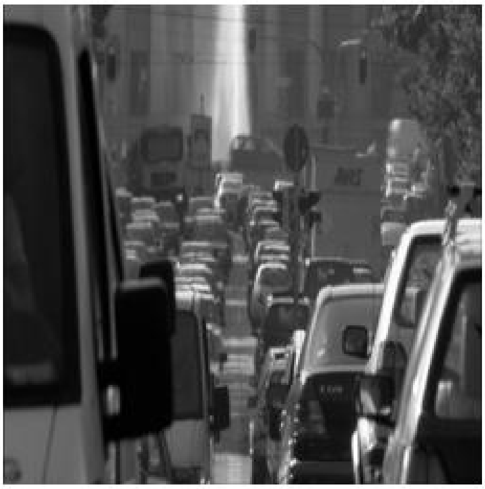


Fig. 10 The original frame.

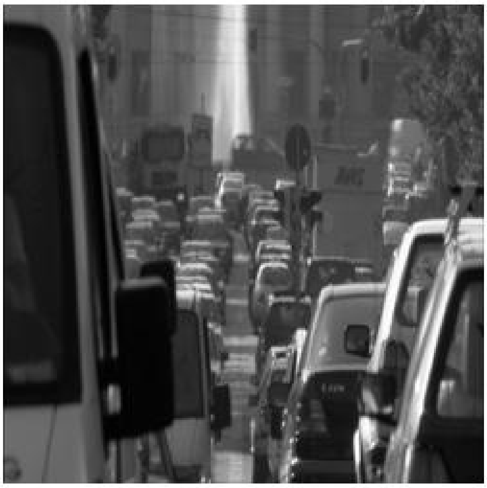


Fig. 11 The watermarked frame.

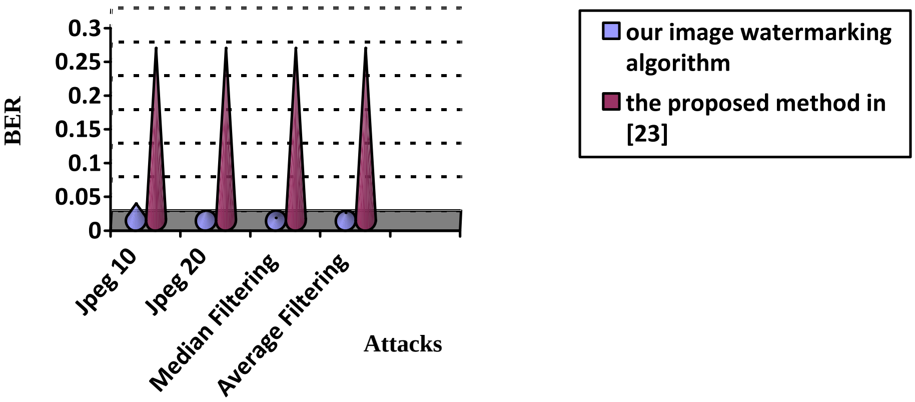


Fig. 12 Comparison results between our proposed image watermarking method and the proposed method in [23].

Table 2 Results of our proposed video watermarking algorithms (the first method means our proposed method in the spatial domain and the second method is our proposed method in the wavelet domain).

Attacks	The first method		The second method	
	PSNR	BER %	PSNR	BER %
N0-attack	48.02	0.00	47.71	0.00
JPEG (QF= 60%)	41.42	0.00	41.34	0.00
JPEG (QF= 40%)	39.53	0.00	39.53	0.00
Rotation 3^o	25.00	0.90	25.00	0.00
Rotation 7^o	21.46	2.10	21.00	4.00
Salt & Pepper (0.01)	24.80	0.40	24.91	6.00
Median Filter [3 3]	40.24	0.00	40.19	4.00

Table 3 Comparison results between our proposed image watermarking method and the proposed method in [9]. (logos used in Red, Green, and Blue components called a, b, and c respectively).

Attacks	Our proposed image watermarking				The proposed method in [9]			
	PSNR	BER %			PSNR	BER %		
		a	b	c		a	b	c
Median Filter [3 3]	33.70	0.00	0.00	0.00	25.30	45.00	45.00	49.00
Rotation 2^o	23.10	1.10	0.00	0.00	23.82	28.00	27.00	21.00

Table 4 Comparison results between our proposed video watermarking methods and the proposed method in [2].

Attacks	Our proposed method in the spatial domain	Our proposed method in the wavelet domain	The proposed method in [2]
Rotation 1^{o}	1.00	1.00	0.7327
Rotation 2^{o}	1.00	1.00	0.7300
Rotation 3^{o}	1.00	1.00	0.7306
Rotation 4^{o}	1.00	1.00	0.7336
Rotation 5^{o}	1.00	0.9354	0.7322

in which, $w^{'}$ denotes the extracted watermark and w is the original watermark and exponent ^{T} stands for transpose. Again a glance at Table 4 confirms that the proposed method enjoys a better resistance against a rotation attack.

5 Conclusions

This paper sought to deploy chaotic maps in watermarking algorithms and demonstrated that by harnessing two important properties of these maps i.e. sensitivity to initial conditions and being non-periodical, it is possible to achieve a highly resistant watermarking algorithm. The result of comparisons with other methods [2], [9] and [23], have indicated that the proposed approach exhibits impressive robustness. In this paper we have tried to develop techniques that are based on simple algorithms and yet quite resistant to many potential attacks. One notable feature of these innovative proposed methods are that they are highly resistant against compression and rotation attacks.

References

[1] Chandra M. B. and Srinivas K. S., "Robust 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, 2009.

[2] Liu Y. and Zhao J., "A new video watermarking algorithm based on 1D DFT and Radon transform," *Signal Processing* 90, pp. 626–639, 2010.

[3] Deng-Yin Z., Jia-ping C. and Jun-Cai S., "Design and implementation of improved watermarking system in WT domain," *The Journal of China Universities of Posts and Telecommunication*, Vol. 14. Issue 2, June 2007.

[4] Preda R. O. and Vizireanu D. N., "A robust digital watermarking schem for video copyright protection in the wavelet domain," *Measurement* 43, pp. 1720-1726. 2010.

[5] Munawer Al-Otum H. and Abdul Samara N., "A robust blind color image watermarking based on wavelet-tree bit host difference selection," *Signal Processing*, pp. 2498–2512, 2010.

[6] Wu Y. T. and Shih F. Y., "Digital watermarking based on chaotic map and reference register,"*Pattern Recognition* 40, pp. 3753–3763, 2007.

[7] Peng Z. and Liu W., "Color image authentication based on spatiotemporal chaos and SVD,"*chaos, Solitons and Fractals*, pp. 946–952, 2008.

[8] Singh N. and Sinha A., "Digital image watermarking using gyrator transform and chaotic maps," *Optik* 121*,* pp. 1427-1437, 2010.

[9] Behnia S., Teshnelab M. and Ayubi P., "Multiple-watermarking schem based on improved chaotic maps," *Commun Nonlinear Sci Numer Simulat* 15, pp. 2469–2478, 2010.

[10] Wu X. and Guan Z.-H., "A novel digital watermark algorithm based on chaotic maps," *Phys. Lett.* A 365*,* pp. 403–406, 2007.

[11] Ni R., Ruan Q. and Zhao Y., "Pinpoint authentication watermarking based on a chaotic system," *Forensic Science Internationa*l 179*,* pp. 54–62 ,2008.

[12] Chen S. and Leung H., "Chaotic watermarking for video authentication in surveillanc applications," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 18, No. 5, May 2008.

[13] Mobasseri B., Sieffert M. and Simard R., "Content authentication and tamper detection in digital video, " *in Proceeding of IEEE International Conference on Image Processing*, Vol. 1, pp. 458-46, 2000.

[14] Lee C. and Lee H., "Geometric attack resistant watermarking in wavelet transform domain," *Optics Express,* Vol. 13, No. 4, pp.1307-1321, 2005.

[15] Dawei Z., Guanrong C. and Wenbo L., "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos Solitions Fractals 22,* pp. 47-54, 2004.

[16] Choi D., Do H., Choi H. and Kim T., "A blind Mpeg-2 video watermarking robust to camcorder recording," *Signal Processing* 90, pp. 1327-1332, 2010.

[17] Koz A. and Alatan A. A., "Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System," *IEEE Transactions on Circuits and Systems for Video*

Technology, Vol. 18, No. 3, pp. 326-337, March 2008.

[18] Ye D., Zou C., Dai Y. and Wang Z., “A new adaptive watermarking for real-time MPEG videos, ” *Applied Mathematics and Computation* 185, pp. 907-918, 2007.

[19] Zhang J., Ho A., Qju G. and Marziliano P., “Robust video watermarking of H.64/AVC,” *IEEE Transactions on Circuits and System-II: Express Briefs* 54, pp. 205-209, Feb. 2007.

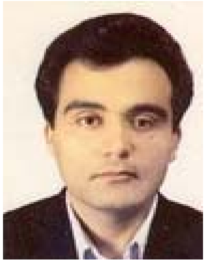
[20] Mobasseri B. G. and Cinalli D., “Lossless watermarking of compressed media using reversibly decodable packets, ”*Signal Processing* 86, pp.951–961, 2006.

[21] Kim H., Baek Y., Lee H. and Suh Y., “Robust image watermark using Radon transform and bispectrum invaraints,” *Lecture Notes in Computer Science*, Vol. 2578, pp. 145–159, 2003.

[22] Kathleen T. Alligood, Tim D. Sauer and James A. YorkeA., “*Chaos: An Introduction to Dynamical systems*”, Springer, New York, 2001.

[23] Guang G. and Guo-ping J., "Zero-Bit watermarking resisting geometric attacks based on composite-chaos optimized SVR model", *The Journal of China Universities of Posts and Telecommunications*, pp. 94-101, April 2011.

Somayyeh Mohammadi has received B.Sc. and M.Sc. in Electrical Engineering from Shahid Bahonar University of Kerman, Iran, in 2008 and 2011, respectively. She has published several papers during her M.Sc. studies in image and video watermarking. Her current research interests are in image and video processing, especially in design of image and video watermarking systems.



Siamak Talebi received B.S. and M.S. degrees, both in Communication Engineering, from Isfahan University of Technology, in 1989 and 1992 respectively and a Ph.D. degree from the University of London (King’s College), in 2001. He is currently with the Department of Electrical Engineering at Shahid Bahonar University of Kerman, in Iran. He is also with the Advanced Communications Research Institute at Sharif University of Technology, Tehran, Iran. His research interests are wireless communications, cognitive radio, MIMO-OFDM and also video coding.

Ahmad Hakimi has received a B.S. degree in Electrical Engineering from Shahid Bahonar University of Kerman, Iran, in 1986 and M.S. and Ph.D. degrees from Istanbul Technical University (ITU), Turkish, in 1995 and 1996 in the field of high-frequency electronics. He is currently with the Department of Electrical Engineering at Shahid Bahonar University of Kerman, Iran. His research interests include the design and analysis of nonlinear RF circuits and image processing.