8th International ISC Conference on Information Security and Cryptology (ISCISC'11)
Ferdowsi University of Mashhad-September 14-15, 2011

A Secure and Robust Video Watermarking Based on Chaotic Maps

Somayyeh Mohammadi[1], Siamak Talebi[2], and Ahmad Hakimi[3]
Department of Electrical Engineering Shahid Bahonar University of Kerman, Kerman, Iran
[1]mohammadi_0313@yahoo.com, [2]siamak.talebi@mail.uk.ac.ir,[3]hakimi@mail.uk.ac.ir

***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 arrive at a like-noise signal. This approach makes extraction of the watermark signal for potential attacker very hard. Embedding locations are selected based on certain principles. The experimental results demonstrate that our proposed watermarking method is highly superior to other techniques and readily achieves the desired robustness and security level.**

Keywords-chaotic maps; robustness; security; watermarking.

I. INTRODUCTION

Recently, with exorbitant growth of internet networks and multimedia technology such as image, voice, and video information exchanges we are increasingly witnessing passage 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 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. Of course, with video content there is another main attack called collusion attack. 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, such that the more the keys the securer the method. 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. As we all know, most of the times there is a trade-off between these different factors which depending on applications we keep a factor in an ideal stage.

In order to have a highly secure video watermarking method, it is desirable to use chaotic maps. Different watermarking schemes based on chaotic maps have been proposed for images [1]–[4], but few for videos [5].

In this paper, we focus on applications of chaotic maps for video watermarking. We encrypt a binary watermark into a tent map [1] to have a like-noise signal.

All video watermarking methods are categorized into two domains: uncompressed domain [6]–[10] and compressed domain [11], [12]; in which the uncompressed domain can in turn be divided into spatial domain [10] and transform domain [6]–[9]. Methods based on uncompressed domain are independent of compression standard being applied whereas we in our study 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 IV verify its robustness for JPEG compression.

The video watermarking algorithm in [6] 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 [7] 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 [8] 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 [13], the scale invariant feature transform feature is used to generate circular patches as the embedding units. In [14], 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 [15], 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. The rest of the paper is organized as follows:

In section II we take a look at chaotic maps and present our proposed method in section III. 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 IV. The paper in its concluding section outlines the advantages of the proposed technique highlighting its resiliency and potentials to overcome many key challenges facing watermarking systems including security and cumbersome computational requirements.

II. CHAOTIC MAPS

Chaos identifies itself with non periodicity, a phenomena which is sensitively dependent on initial conditions [16]. Dependence on initial conditions refers to the property that pairs of points "which begin as close together as desired" will eventually move apart, namely 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. Let's see how these translate 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 [16]:

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

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

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

If this limit exists. Notice that h exists if and only if L exists and that 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 [16]:

$$T_a(x) = \begin{cases} ax & if\ x \le 1/2 \\ a(1-x) & if\ x \ge 1/2 \end{cases} \qquad (3)$$

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 $1 \le a \le 2$, 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.

III. 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 never the less these frames are compressed somewhat lower than P-frames and B-frames and we select I-frames for watermark embedding. Also the embedding is performed in Y components of I-frames. 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:

A. Watermark Generation

We construct a chaotic sequence by a tent map which is defined as [1]:

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

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

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

Where m, is the frame's number. Now we rewrite (4) for a bipolar sequence as:

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

Where x_n is chaotic sequence that constructed from (4) and $x_{n,new}$ is the resulted bipolar sequence includes -1 or 1. Our concern here is to encrypt the binary logo image in (6). Let the binary logo be $g(x, y)$. We convert $g(x, y)$ to a bipolar one dimensional sequence and multiply this sequence by (6). The resulting sequence called $w(x)$ is the chaotic watermark and constitutes a like-noise signal. Of course, to embed $w(x)$ into Y component, we have to make changes to $w(x)$ which we elaborate how this is done in the next sub-section. Note that the number of iterations (n) corresponds to the size of logo image.

B. Watermark Embedding

We select the Y components of I-frames for embedding the generated watermark in the previous sub-section. The block diagram of watermark embedding is shown in Fig.1. The watermark embedding is performed in spatial domain and the steps as follows:

- 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 as β_1 and β_2 such that $\beta_1 < \beta_2$, and we save these locations as keys. Now we dedicate β_1 and β_2 to the chaotic watermark as bellow:

$$w(x)_{new} = \begin{cases} \beta_1 - \varepsilon & if\ w(x) = -1 \\ \beta_2 - \varepsilon & if\ w(x) = 1 \end{cases} \quad (7)$$

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 resilient 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 (7), as found in (8) or (9), transparency will be increased.

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

Or

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

In fact, using (7) , (8) or (9) we convert the bipolar chaotic watermark $w(x)$ into a sequence $w(x)_{new}$ comprising $[\beta_1 or \beta_1 - \varepsilon, \beta_2 or \beta_2 - \varepsilon]$ 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 is $\beta_1 or \beta_1 - \varepsilon$, then we embed it into a location of the frame where its luminance was β_1 , and if the watermark is $\beta_2 or \beta_2 - \varepsilon$ then we embed it into the location where its luminance was β_2 . 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 not possible.

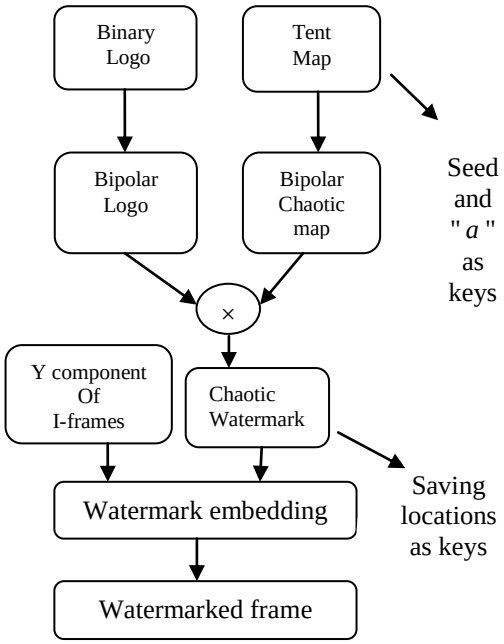

Figure 1. Block diagram of watermark embedding.

C. Watermark Extraction

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

1. We should 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:

$$p(x) = \begin{cases} -1 & if\ |g(x) - \beta_1| \le |\beta_1 - \beta_2|/2 \\ 1 & other\ else \end{cases} \quad (10)$$

Where $g(x)$, is the extracted luminance value and $p(x)$ is the bipolar sequence resulting from (10).

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:

$$q(x)=\begin{cases}0 & if\ w'(x)=-1\\ 1 & if\ w'(x)=1\end{cases} \quad (11)$$

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

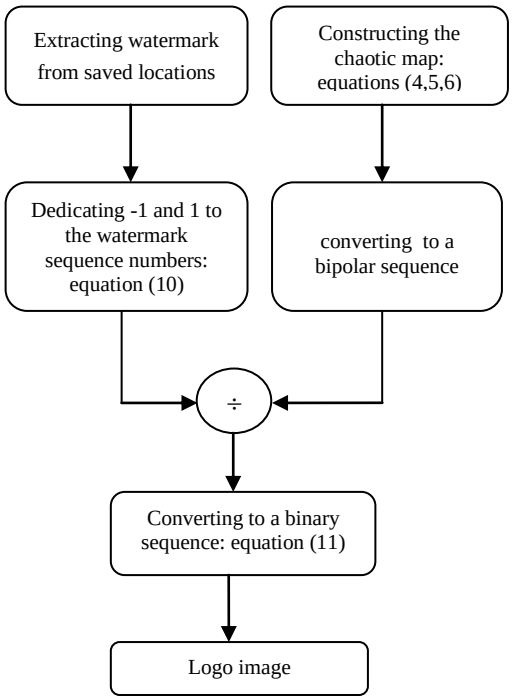

Figure 2. Block diagram of obtaining the logo

IV. Experimental Results

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.

A. Simulation Results of Our Proposed Method

The logo is just a binary image (50×50) which is illustrated in Fig. 3d, and details of the video sequences utilized in the simulation, β_1, and β_2 values have been written in Table I. 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 II. Distortion in an I-frame is measured by Peak Signal to Noise Ratio (PSNR) and we utilize Bit Error Rate (BER) to determine how the extracted logo is similar to an original logo. The following relation calculates the BER.

$$BER=\frac{B}{m\times n} \quad (12)$$

Where B denotes the number of erroneously detected bits and $m\times n$ is the extracted binary watermark image dimensions. Parameters 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. The original I-frames and the watermarked I-frames are shown in Fig. 3. It can be seen from Fig. 3, that the watermarked frames are visually as crisp as the original ones. As we mentioned before, in our method the watermark embedding is performed in spatial domain therefore, we need to confirm that the method is robust against compression attacks. It is clear from Table II, that there should be no concern about JPEG compression. Also from this table, it is observed that our method has high resilience against filtering, rotation, and salt & pepper noise. Fig. 4, illustrates the extracted logo for pedestrian video after applying some attacks. Note that in order to extract the logo from the rotated image, we 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.

B. Comparison Results

In this sub-section, we comprise resistance of our method with methods in [6] and [15]. The first comparison is between our method with method in [6]. In this comparison, the comparison parameter is considered as normalized correlation value and is calculated as follow:

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

In which, 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 Table III. With respect to the Normalized correlation values achieved by our method, it is obvious that our method is resistant versus the rotation attack against watermarking systems in [6].

In another comparison, we comprise our method with the scheme in [15] from view point of PSNR. Of course, it is noticeable to say that both methods in this paper and in [15] have zero BER against different types of filtering attacks. Fig. 5, shows the comparison results. From this figure, it is clear that our method has more transparency.

V. Conclusion

A simple video watermarking algorithm with high resilience is proposed based on chaotic maps. The research devotes itself to the study of spatial domain watermarking and discovers it exhibits potent defense against many unintended

or malicious attacks (Table II). To make the technique immune against collusion attacks embedding of different watermarks in different frames were carried out with good results. 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 [6] and [15].

TABLE I. 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

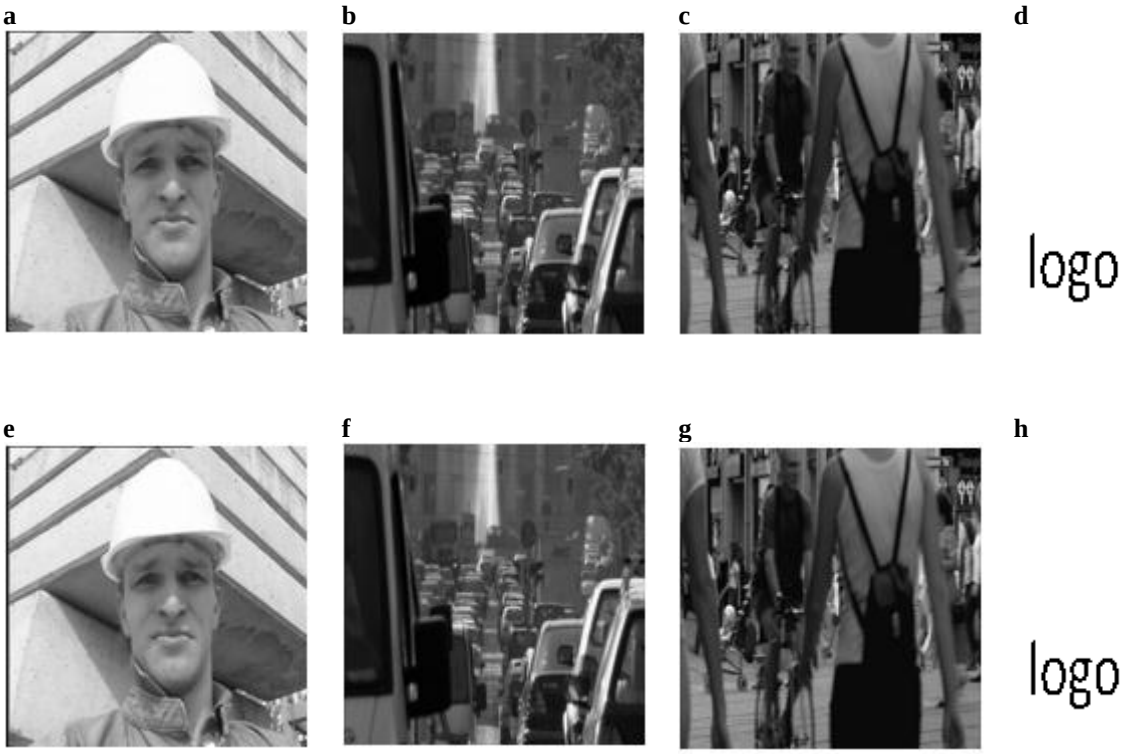

Figure 3. (a), (b), and (c) are original frames. (d) is the original binary logo. (e), (f), and (g) are the watermarked frame. (h) is the extracted logo.

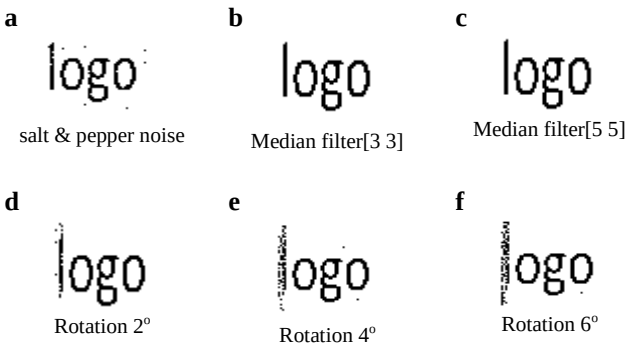

Figure 4. The extracted logos under different attacks.

TABLE II. 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 III. COMPARISON RESULTS BETWEEN OUR METHOD AND METHOD IN [6]. (THE TEST VIDEO IS FLOWER-GARDEN (SIF)).

Attacks	Our proposed method	Proposed method in [6]
	sim	sim
Rotation 1°	0.9955	0.6551
Rotation 2°	0.9888	0.6270
Rotation 3°	0.9644	0.6334
Rotation 4°	0.9555	0.6280
Rotation 5°	0.9733	0.6251

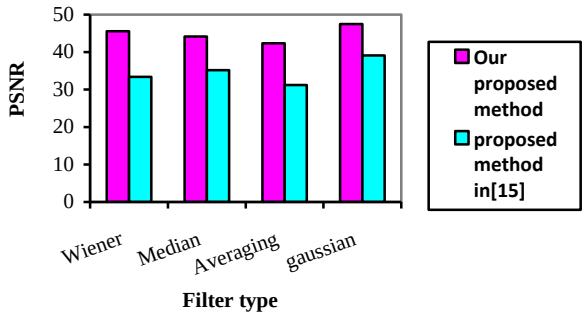

Figure 5. Comparison results between our method and method in [15], from PSNR view point, under different types of filtering (BER under these filters is zero for both methods). (The test video is Rush Hour).

REFERENCES

[1] Narendra Singh, Aloka Sinha, "Digital image watermarking using gyrator transform and chaotic maps," Optic 121, pp. 1427-1437, 2010.

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

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

[4] Rongrong Ni, Qiuqi Ruan and Yao Zhao, "Pinpoint authentication watermarking based on a chaotic system," Forensic Science International 179, pp. 54-62 ,2008.

[5] Siyue Chen and Henry Leung, "Chaotic watermarking for video authentication in surveillanc applications," IEEE Transactions on circuits and systems for video technology, vol. 18, no. 5, May 2008.

[6] Yan Liu, Jiying Zhao, "A new video watermarking algorithm based on 1D DFT and Radon transform," Signal Processing 90 (2010) 626-639.

[7] Radu O. Preda and Dragos N. Vizireanu, "A robust digital watermarking schem for video copyright protection in the wavelet domain," Measurement 43 (2010) 1720-1726.

[8] Dooseop Chio, Hoseok Do, Hyuk Choi and Taejeong Kim, "A blind Mpeg-2 video watermarking robust to camcorder recording," Signal Processing 90 (2010) 1327-1332.

[9] 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, vol. 18, no. 3, March 2008.

[10] B. Mobasseri, M. Sieffert and R. Simard, "Content authentication and tamper detection in digital video, " Proceeding of IEEE International Conference on Image Processing, vol. 1, 2000, pp. 458-461.

[11] Dengpan Ye, Changfu Zou, Yuewei Dai and Zhiquan Wang, "A new adaptive watermarking for real-time MPEG videos, " Applied Mathematics and Computation 185 (2007) 907-918.

[12] J. Zhang, A. Ho, G. Qju and P. Marziliano, "Robust video watermarking of H.64/AVC," IEEE Transactions on Circuits and System-II: Express Briefs 54 (February) (2007) 205-209.

[13] L. Hae-Yeoun, K. Hyungshin, L. Heung-Kyu, Robust image watermarking using local invaraint features, Optical Engineering 45(2006) 37001-37002.

[14] Hefei Ling, Liyun Wang, Fuhao Zou, Zhengding Lu, Ping Li, "Robust video watermarking based on affine invariant regions in the compressed domain,"Signal Processing 91 (2011) 1863- 1875.

[15] 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, vol .3, no .3, Sep 2008.

[16] Kathleen T. Alligood, Tim D. Sauer and James A. Yorke, Chaos: An Introduction to Dynamical systems. Springer, New york,2001.