A Novel Video Watermarking Method Using Visual Cryptography

Amir Houmansadr
Department of Electrical Engineering,
Sharif University of Technology, Tehran, Iran
houmansadr@ee.sharif.edu

Shahrokh Ghaemmaghami
Electronics Research Center,
Sharif University of Technology, Tehran, Iran
ghaemmagh@sharif.edu

Abstract-**In this paper we propose a novel approach to insertion of watermark in the video sequences. The proposed scheme is based on visual cryptography and performs temporal scrambling for watermark embedding. Watermark, which may be a visible logo, is frequently split and inserted into video frames. Watermark detection can be verified by the human eye. Inserted watermark is expected to resist collusion attack, which is a major concern in video watermarking. Experimental results show that the proposed method provides a high resilience against some non-hostile video processing schemes, such as geometrical distortions.**

Keywords- Video Signal, Digital Watermarking, Visual Cryptography.

I. Introduction

Nowadays, digital watermarking has found useful applications in different areas. In design of multimedia intelligent systems, an appropriate mechanism should be used to accompany necessary information with the media, regarding various purposes. A surveillance camera, for example, should insert a digital signal into the video signal to prepare information such as the originality of the recorded media, camera ID, time stamp, and other parameters of the system which can be of a vital value. Digital watermarking is a good means to satisfy the desired functionalities.

A digital watermark is basically an invisible mark that is inserted into a digital media such as audio, image, or video, which is used to identify illegal distributions of copyright protected digital media and also lawbreaking customers. A digital watermark should have certain features to achieve desired functionalities. The embedded mark is to be robust enough against various watermarking attacks, while keeping the perceived quality of the host image unchanged (the imperceptibility requirement). Watermarking attacks consist of deliberate attacks made maliciously to remove or change the mark sequence by lawbreakers and unintentional attacks caused as a result of different kinds of coding and compression made to the digital media prior to transmission and/or storage and also errors occurred during the transmission of the media through networks [1].

Video contents can be mentioned as the most valuable digital media, which are increasingly used illegally, resulting in a huge damage to filmmaking industry. Video watermarking is utilized for different video applications [1], [2]. Historically, *copyright protection* is the first targeted application of digital watermarking. To do this, a digital mark is embedded into the digital contents to prove the paternity of the copyright owner. Copyright protection has been investigated for video watermarking in different manners [3]. *Copy control* is the other video watermarking application. By the demand of copyright owners and Hollywood studios, the Copy Protection Technical Working Group (CPTWG) defined a system for future DVD (Digital Versatile Disk) devices in order to prevent illegal copying of DVD disks [4]. One of the six components of this system obligates compliant devices to check for a copy authorization watermark in the MPEG-4 video streams before playing and/or recording digital video sequences on DVDs. As another video watermarking application, *Fingerprinting* enables digital media producers to trace back the traitor customers whom have distributed copyrighted media with no permission through some peer-to-peer systems (e.g. ShareAza, KaZaA, eDonkey) by inserting an indelible and invisible watermark identifying the corresponding customer. This also can be done for Pay-Per-View (PPV) and Video-On-Demand (VOD) services by inserting the customer's ID into the delivered video data [5]. Other applications exist for video watermarking, such as *Broadcast Monitoring* [6], *Video Authentication* [7] and *Enhanced video coding* [8], as the most popular ones.

As long as video watermarking is concerned, special challenges must be considered [1], [2]. Various non-hostile video processing schemes such as photometric attacks, spatial and temporal desynchronization and different video editing schemes alter the performance of watermarking algorithms. In addition, inter-videos collusion and intra-video collusion of malicious users to gain the non-watermarked video sequences are important issues in the case of video watermarking, because of twice opportunities to make such an attack in this area. Real-time implementation is the other constraint that some of video watermarking algorithms have to take into account.

In this paper, we propose a novel video watermarking scheme, which is robust to collusion attacks. Our scheme is based on the concept of visual cryptography, which was initially introduced by *Naor* et al. [9]. A visible mark (which can be a logo of the owner) is split frequently according to a (2,2) secret sharing scheme and then inserted into the frames of the video in a confidential manner. The proposed scheme is also robust to some nonhostile video processing schemes. In

This research is supported in part by Iran Telecommunications Research Center (ITRC).

1-4244-0457-6/06/$20.00 ©2006 IEEE

section 2 we present a brief overview on the concept of visual cryptography. The proposed embedding and detection algorithms are described in section 3. Section 4 discusses the experimental results and section 5 concludes the paper.

II. Visual Cryptography

In 1979, *Blakly* and *Shamir* independently developed the concept of *secret sharing* [10], [11]. A secret sharing scheme shares a secret into a number of shares so that the cooperation of a predetermined group of shareholders reveals the secret, while the secret reconstruction is impossible to any unauthorized set of shareholders. Visual cryptography is a kind of secret sharing in which the secret reconstruction can be done only by the human visual system [9]. This is why it is also called visual secret sharing (VSS).

Many VSS schemes have been introduced in the literature, where we consider the (2,2) VSS scheme proposed by Naor et al. in [9]. According to the algorithm, each pixel of the binary-valued secret image is expanded into 2*2 pixels, as shown in table 1. To share a white pixel in the secret image, one row from the first 6 rows of table 1 is chosen randomly. Similarly, two shares of a black pixel are determined by a random selection from last 6 rows of table 1. As a result, an M*N pixels secret image is expanded into two (2M)*(2N) sharing images.

TABLE 1
A (2x2) VSS Scheme Using 2x2 Subpixels.

Secret Pixel	Share1	Share2	Stacked
White	■□ □■	■□ □■	■□ □■
	□■ ■□	□■ ■□	□■ ■□
	■□ ■□	■□ ■□	■□ ■□
	□■ □■	□■ □■	□■ □■
	□□ ■■	□□ ■■	□□ ■■
	■■ □□	■■ □□	■■ □□
Black	■□ □■	□■ ■□	■■ ■■
	□■ ■□	■□ □■	■■ ■■
	■□ ■□	□■ □■	■■ ■■
	□■ □■	■□ ■□	■■ ■■
	□□ ■■	■■ □□	■■ ■■
	■■ □□	□□ ■■	■■ ■■

Considering security of the method, presence of only one sharing image reveals nothing about the corresponding secret image, i.e. each 2*2 pixels of one sharing image may correspond to either a white pixel or a black pixel of the secret image.

As table 1 shows, stacking the shares of a black secret pixel results in 4 black subpixels, while only 2 black subpixels is gained by stacking shares of a white secret pixel. So, secret image is revealed to human eye by stacking the shares without performing any cryptographic computation. Fig. 1 shows the result of superimposing the share images of a secret image. Original secret image can be obtained using a simple reduction algorithm from the superimposed image.

In the next section, the mentioned (2,2) VSS scheme is utilized in the proposed watermarking algorithm.

III. Embedding And Detection Algorithms

In this section we utilize the (2,2) VSS scheme mentioned above to frequently split the watermark image (logo) into pseudo-random shares. As mentioned before, each pixel in the secret image can be split in 6 different manners. As a result, there are 6^{M*N} alternatives to share an M*N pixels secret image, so selecting two sharing images from two different executions of the VSS algorithm reveals nothing about the secret image.

We transform the watermark (binary logo) and all the shares from binary (0,1) to signed format (-1,+1), which leads an approximately zero-mean pseudo-random watermark sequence, so we perform the detection process in a correlation-based manner. Fig. 2 illustrates the proposed embedding scheme. First, the video sequence to be marked is temporally scrambled (by changing the order of frames) using an m-sequence produced by a Linear Feedback Shift Register (LFSR) [12]. A simple modular scrambler can be used instead, with lower security, by permuting the position of the frames as below:

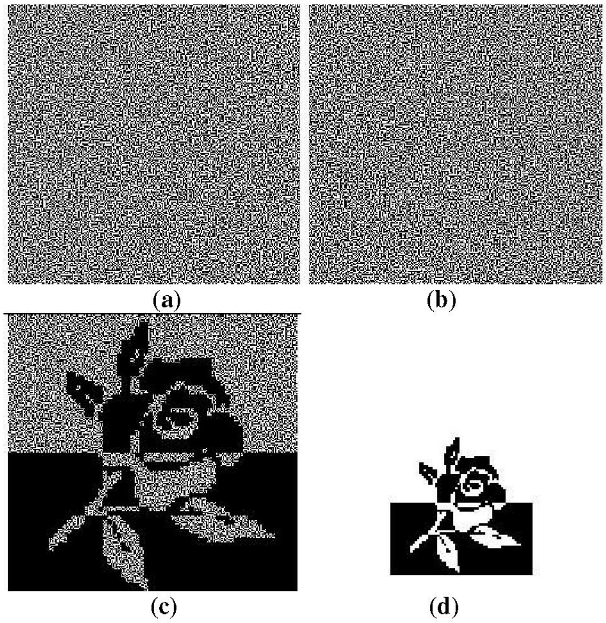
$$u=mod(p.i,L)+1, \qquad (1)$$

where u is the scrambled position of i-th frame, L is the length of the video sequence and mod(x,y) is the modular residue of x in respect to y. Mathematically, if p is an integer number which is prime relative to L, (1) makes an one-to-one relationship between the original video frames and the scrambled video frames.

Then the insertion stage performs on the frames of this scrambled video sequence as below:

$$\begin{aligned} F_{s,w}(2k-1) &= F_s(2k-1)+\alpha.SH1(k), \qquad (2)\\ F_{s,w}(2k) &= F_s(2k)+\alpha.SH2(k), \qquad k=1,\dots,[L/2] \end{aligned}$$

where $F_s(x)$ is the x'th frame of the temporally-scrambled video sequence, $F_{s,w}(x)$ is the x'th temporally-scrambled and watermarked frame, *SH1(k)* and *SH2(k)* are the shares of the logo in the *k*'th run of the VSS algorithm, α is a parameter defining watermark's strength (we set it equal to 3), and L is the number of frames of the video sequence. Initial condition of the LFSR, S, (or p in the modular scrambler) serves as the private key in the watermark detection stage. A reverse temporal-scrambling produces the final video sequence, F_w.


(a) (b)

(c) (d)

Fig. 1. Stacking two share images of a secret image. (a): first share, (b): second share, (c) stacked shares without reduction and (d): reducing stacked image which is the same as split secret image (Fig. d from [1])

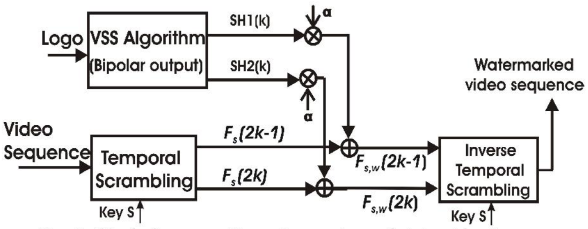


Fig. 2. Block diagram of inserting watermark into video frames.

Fig. 3 depicts the detection process of the watermarked sequence. First, all frames of the received video stream (F_w) pass through a spatial High Pass Filter (HPF) for the aim of strengthening the high-frequency pseudo-spread spectrum watermark sequence in the frames. The resulting video sequence gets temporally scrambled to make the frames containing corresponding shares adjacent. For k=1,..,[L/2], the *Stack* function acts on the $F_{w,f,s}(2k-1)$ and $F_{w,f,s}(2k)$ frames of the resulting sequence which yields [L/2] stacked frames (F_{st}). Fig. 4 shows the block diagram of the defined Stack function. The first block gives the pixel-by-pixel minimum of the two frames, which is followed by a block that results in a half-sized image by returning the maximum value of each 2*2 pixels block. It can be easily shown that the defined stack function retrieves the split binary logo from its VSS shares.

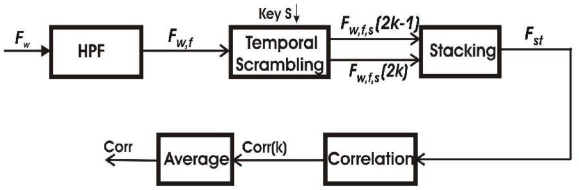


Fig. 3. Block diagram of watermark detection.

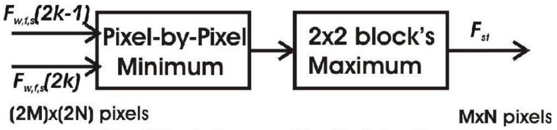


Fig. 4 Block diagram of the Stack function.

Using the concept of spread spectrum watermark detection, each of the [L/2] stacked frames gets correlated by the signed logo as below:

$$Corr(k) = \frac{F_{st}(k) \bullet W}{\sqrt{E(F_{st}(k)) * E(W)}}, \ k = 1, \ldots, [\frac{L}{2}] \quad (3)$$

where W is the signed logo, $E(F)$ returns the energy of frame F, and the dot represents the inner production. An average on these correlations gives a measure (*Corr*) to decide whether the received video sequence contains the specified watermark or not.

If the distortion made to the watermarked video sequence is unnoticeable, the mark's existence is also verified by the human eye. This is because F_{st} visually resembles the watermark logo. Fig. 5 shows the F_{st} and the corresponding watermark logo, when just a little distortion is made to the watermarked sequence.

One can observe the owner's logo by exhaustively stacking filtered video frames. However, he/she can not remove the inserted watermarks, which are sharing images of this logo. If confidentially of this logo is desired, spatial-scrambling (permuting pixels of the frames) can be performed on the sharing images in the watermark insertion stage.

IV. Experimental Results

We simulated the proposed embedding and detection schemes to investigate the resilience against various challenges. We tried different HPFs to maximize the ratio of true detection (correlation by the correct watermark) to false

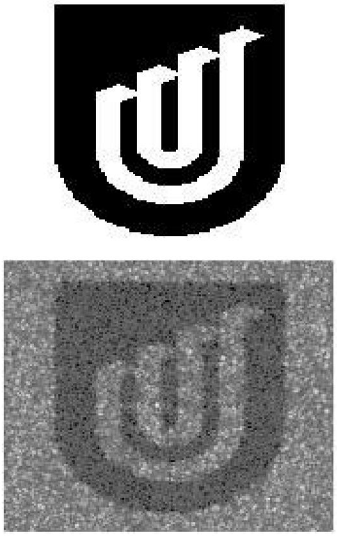


Fig. 5. Visual similarity of the stacked image and the watermark logo

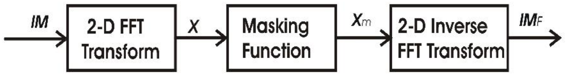


Fig. 6. Block diagram of the FFT filtering.

detection (correlation by a non-relevant watermark). The ratio is maximized using an FFT filter whose normalized cut-off frequency is about 0.31. Fig. 6 shows the block diagram of an FFT filter. The two-dimensional FFT transform of the video frame is passed through a masking stage which drops its low-frequency components and then an inverse two-dimensional FFT transform is performed.

Using the mentioned FFT filter in the detection scheme, the average ratio of true detection to false detection is about 8, depending on the watermark logo. Fig. 7 shows the correlation evaluated by the watermark detector, between the watermark logo and randomly stacked video frames. The peak value belongs to the true stacking.

A. Collusion Attack

In video watermarking, much more data is available to both attacker and watermarker, as compared to image watermarking. This makes collusion attack a serious concern in video watermarking.

For a set of watermarked frames $X_k=F_k+\alpha_k W_k$, $k=1,..,L$ and their corresponding video frames F_k , the linear collusion attack is made as below:

$$\overline{X} = \sum_{k=1}^{L} \beta_k X_k = \sum_{k=1}^{L} \beta_k F_k + \sum_{k=1}^{L} \beta_k \alpha_k W_k \ , \qquad (4)$$

where W_k is the watermark sequence and β_k is a weighting coefficient. $\overline{X}$ gives an optimal MSE (Mean Squared Error) estimate of the watermark or the host signal depending on the type of collusion [13].

The video watermark W is statistically invisible, if and only if the correlation coefficient between every two video frames F_a and F_b is equal to that of the corresponding watermarked frames X_a and X_b [13]:

$$Corr(F_a, F_b) = Corr(X_a, X_b). \qquad (5)$$

Simulations show that setting the parameter α in (1) smaller than five satisfies the above condition.

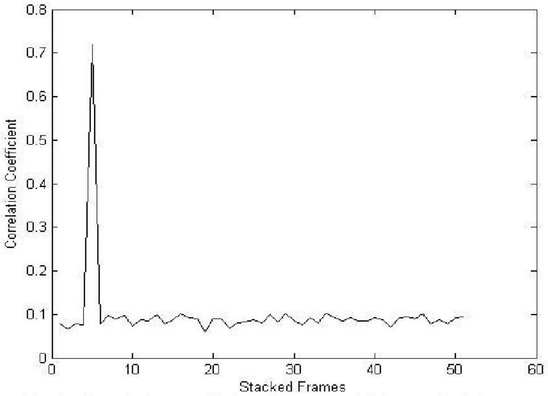


Fig. 7. Correlation coefficient for true and false stacked frames.

Intuitively, we expect the proposed scheme to be robust against collusion attacks. On one hand, in each frame of the video sequence, a different pseudo-spread spectrum watermark is embedded. On the other hand, if the mark is distorted in some still regions of the video stream, the detection algorithm still has a good chance to detect the mark due to the insertion of shares of a same logo throughout the video signal. This makes intra-video collusion impossible.

In [13] it is shown that a sufficient condition for robustness to linear collusion is that for every two frames F_a and F_b and the corresponding watermarked frames X_a and X_b we have:

$$Corr(F_a, X_a) = Corr(F_b, X_b). \qquad (6)$$

Experimental results comply with this condition, assuring the robustness of the proposed scheme to collusion attack.

Also, inserting an additional customer ID watermark in the transform domain makes the inter-videos collusion defeated.

B. Other Attacks

We applied different geometric distortions to the watermarked sequence to see how the detection response alters. In the case of video watermarking, the attacker has to perform the same geometric distortion on all of the frames to keep the continuity of the video sequence. By performing spatial synchronization prior to detection, output of the detection algorithm following various amounts of frame cropping, frame rotating, and changing the Aspect Ratio (AR) showed a high resilience against such distortions. As discussed in section III, decision on the watermark existence is made by evaluating a correlation coefficient. Tables 2 to 4 show the decrement of this correlation coefficient, *Corr*, after performing frame cropping, frame rotating, and changing the AR of the watermarked video sequence, respectively. Also, the watermarking system showed a good resilience to geometric distortions when no synchronization is performed.

This high strength to geometric attacks is due to the VSS compatibility with this kind of distortions. Fig. 8 depicts the result of stacking sharing images, which are distorted as described. Also, as table 5 shows the watermarked video sequence is robust to video resizing (frame scaling).

TABLE 2
DECREMENT OF THE CORRELATION COEFFICIENT AFTER FRAME CROPPING
(KEEPING MIDDLE OF FRAMES)

Cropping Percentage	10	20	30	40	50
Decrement of *Corr* (%)	8	10	6	11	16

TABLE 3
DECREMENT OF THE CORRELATION COEFFICIENT AFTER FRAME ROTATING

Rotation angle	5	10	15	20	25
Decrement of *Corr* (%)	7	6	8	10	9

TABLE 4
Decrement of the Correlation Coefficient After Changing The ar Of 240*360 Pixels Watermarked Frames

New Size(pixels)	240*180	240*90	480*360
Decrement of *Corr* (%)	15	12	29

TABLE 5
Decrement of the Correlation Coefficient after Frame Scaling

Scaling Ratio (R)	2	4	8
Decrement of *Corr* (%)	29	31	39

In addition, pirate attacks such as frame swapping and frame dropping will be defeated, because of its low impact on the average correlation (if temporal synchronization is made). Spatial synchronization can be made by an exhaustive correlation search of the watermark by a correctly stacked frame. On the other hand, temporal synchronization can be made by stacking one frame by some frames around the expected location and finding the maximum correlation by the logo (using the temporal-scrambling key). The mark is also expected to survive other nonhostile video processing schemes, such as photometric attacks and video editing processes. Table 6 depicts the average true to false detection ratio, when the watermarked video sequence is M-JPEG compressed with different quality factors.

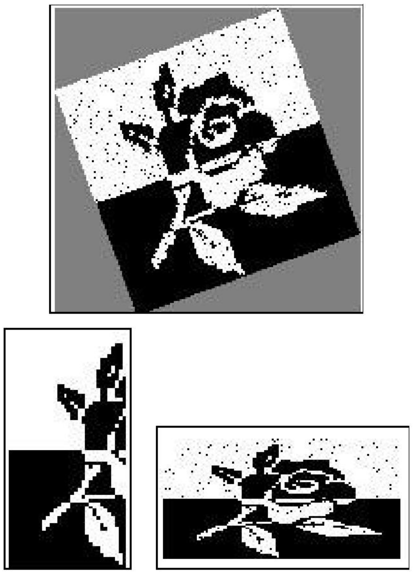


Fig. 8. Retrieving the secret image (watermark) from its geometrical distorted shares. (Top): image rotating, (bottom-left): image cropping and (bottom-right): changing the aspect ratio.

TABLE 6
Average True To False Detection Ratio After M-jpeg Compression For Different Quality Factors

Quality Factor	100	90	80	60	40
Average true to false detection ratio	7.83	5.20	2.75	1.72	1.53

V. Conclusions

In this paper, we have proposed a new watermarking algorithm for video sequences. The proposed scheme is based on the concept of visual cryptography and is performed in the spatial domain. Watermarks to be embedded into frames are shares of the owner's mark (which can be a visible logo) that seem as pseudo-spread spectrum sequences. The detection algorithm relies on the fact that stacking frames, containing corresponding shares of the logo, makes higher correlation with the logo, as compared to stacking frames containing non-relevant shares of the logo. Results show that the proposed method has a high resilience against geometric distortions and other non-hostile video processing schemes. Also, the proposed method can be a countermeasure to collusion attack, which is an important challenge in video watermarking.

Refrences

[1] J. S. Pan, H. C. Huang and L. C. Jain, *Intelligent Watermarking Techniques*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2004.

[2] G. Doer and J. L. Dugelay, "A Guide tour of video watermarking," *Signal processing: Image communications,* Elsevier Science, vol. 18, 2003, pp. 263-282.

[3] S. Craver, N. Memon, B. Yeo ,M. Yeung, "Can Invisible watermarks resolve rightful ownership?," *Technical Report RC 20509,* IBM Research Division, 1996.

[4] J. Bloom, I. Cox, T. Kalker, J.-P. Linnartz, M. Miller, and C. Traw, "Copy protection for DVD video," Proceedings *of the IEEE,* vol. 87 (7), 1999, pp. 1267–1276.

[5] E. Lin, C. Podilchuk, T. Kalker, E. Delp, "Streaming video and rate scalable compression: what are the challenges for watermarking?," *Proceedings of SPIE 4314,* Security and Watermarking of Multimedia Content III, 2001, pp. 116–127.

[6] D. Kilburn, Dirty linen, "Dark secrets," Adweek, 38 (40), 1997, pp. 35–40.

[7] B. Mobasseri, M. Sieffert, R. Simard, "Content authentication and tamper detection in digital video," *Proceedings of the IEEE International Conference on Image Processing*, Vol. 1, 2000, pp. 458–461.

[8] D. Robie, R. Mersereau, "Video error correction using data hiding techniques," *Proceedings of the IEEE Fourth Workshop on Multimedia Signal Processing*, 2001, pp. 59–64.

[9] M. Naor, and A. Shamir, "Visual Cryptography," *Advances in Cryptology - Eurocrypt'94 Proceeding, LNCS* Vol. 950, Springer-Verlag, 1995, pp. 1-12.

[10] G. Blakley, "Safeguarding cryptographic keys," in:Merwin R.E., Zanca, J.T., Smith, *Proceedings of National Computer Conference*, 48, AFIPS Press, New York, 1979.

[11] A. Shamir, "How to Share a secret," *Communications of the ACM,* vol. 22, 1996, pp.612-613.

[12] K. Su, D. Kundur and D. Hatzinakos, " A novel approach to collusion-resistance video watermarking," *Proceedings of SPIE Security of Watermarking of Multimedia contents IV,* San Jose, CA, 2002, pp. 491-502.

[13] R.L. Pickholtz, D.L. Schilling, and L.B. Milstein, "Theory of spread spectrum communications. A tutorial," *IEEE Transaction on Communication,* vol. 30(5), May 1982, pp. 855-884.