2010 IEEE International Symposium on Multimedia

# NoMark: A Novel Method for Copyright Protection of Digital Videos Without Embedding Data

Aditya Vashistha, Rajarathnam Nallusamy, and Sanjoy Paul
*Convergence Lab, Software Engineering and Technology Labs*
*Infosys Technologies Limited, Bangalore, India 560100*
*Email: {aditya_vashistha, rajarathnam_n, sanjoy_paul}@infosys.com*

***Abstract*—Copyright protection of digital media content is becoming increasingly important with increasing potential for content monetization which is attributable to digital convergence. High volumes of uploaded content in social networking and media sharing sites makes it increasingly difficult to monitor all the uploaded content for copyright infringement, piracy and illegal distribution. Currently, digital watermarking is predominantly used for copyright protection of images and videos. Watermarking involves embedding data into an image or a video in an invisible or visible manner. This traditional method is prone to many known watermark attacks aimed at detecting and distorting or destroying the embedded data. In this paper, we present the *NoMark Method*, a robust, reliable, and efficient scheme for copyright protection of digital video content without embedding any data in to it. The method is based on visual cryptography and can be used to watermark individual scenes in a video and hence protects not only the copyright of complete video but also of each individual scene in the video. The method is robust against video fragmentation attack, unauthorized insertion of scenes from a protected video into another video and various other video watermarking attacks. There is no involvement of any notary agency to establish copyright ownership of a digital video.**

***Keywords*-video content protection; visual cryptography; scene change; averaged scene image;**

## I. INTRODUCTION

The Internet is growing enormously due to the convergence of mobile and telecast networks and services with that of the Internet. IPTVs, smartphones, and other consumer electronic devices are joining the Internet as end nodes. This provides immense opportunity for digitization and monetization of media content. Services such as Video-on-Demand (VoD) are no longer limited to Set-Top Boxes and television sets. In addition to the rising viewers of traditional television sets, access to media content from mobile phones are on the rise because of *anytime anywhere* viewing capability [1]. However, this increase in easy access puts digital content at the risk of illegal copying and redistribution through peer-to-peer (P2P) file-sharing systems, websites that accept user-generated content (UGC) or copies in CDs and DVDs. 95 per cent of music downloads are unauthorised, with no payment to artists and producers as per the Digital Music Report published by International Federation of the Phonographic Industry (IFPI), which represents the recording industry worldwide with some 1400 members in 66 countries and affiliated industry associations in 45 countries [2]. According to a study conducted by Motion Picture Association of America (MPAA), the loss to MPAA studios was $6.1 billion to piracy in 2005. Of this $2.3 billion is attributed to Internet piracy alone [3]. As per the 2010 IFPI Digital Music Report, illegal film streams and downloads account for 40% of the film industry's piracy problem by volume.

This growing economical threat to the copyright holders lead to several protection initiatives since the birth of the Internet. World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) adopted in Geneva on December 20, 1996, the US Digital Millennium Copyright Act of 1998, European Esprit project named VIVA (Visual Identity Verification Auditor), and UK's Digital Economy Act of 2010 are some of those initiatives aimed at protecting copyright material over digital networks.

In order to protect the copyrighted content from illegal copying and distribution, many techniques have been developed or are being developed. Research communities across the world are striving continuously to improve the copyright protection techniques. Digital watermarking is one such technique predominantly used for copyright and intellectual property rights (IPR) protection. This technique provides copyright protection of media content by embedding data in an invisible or visible manner. In the proposed *NoMark* method, instead of embedding data in to the image or video, data is extracted from the image or video using visual cryptographic technique to construct one secret share of a watermark image.

A comprehensive survey of various watermarking techniques are presented in literature [4], [5] and are classified into three main categories, namely, spatial domain techniques, frequency domain techniques, and feature domain techniques. With the introduction of a new paradigm of cryptographic schemes, called *visual cryptography* or *visual secret sharing* (VSS), by Naor and Shamir [6] in 1994, digital watermarking of images and videos have taken new dimensions, with a new category which can be termed as *visual cryptography based techniques*. A novel method for digital image copyright protection based on visual cryptog-

978-0-7695-4217-1/10 $26.00 © 2010 IEEE
DOI 10.1109/ISM.2010.32

raphy was introduced by Ren-Junn Hwang in 2000 [7]. This method is briefly outlined in Section II-E.

In this paper, we present a method for watermarking video content using *(2, 2)* visual secret sharing scheme in which first visual cryptographic share is created using a secret key, watermark pattern and averaged scene image of the video to be protected during the *NoMark* protection process. Second share is created using the same secret key and averaged scene image of the video to be verified during the *NoMark* verification process. Watermark pattern is constructed by overlapping these two shares during the verification process. This retrieved and the original watermark patterns will be same only if the averaged scene images and the secret key used in verification process are same as those used in the protection process. This principle is used to establish copyright protection over all or selected scenes in a video.

The rest of this paper is organized as follows. Section II briefly outlines the various techniques used in our approach. Proposed *NoMark Method* is presented in Section III along with the protection and the verification processes. Simulation results and discussions are presented in Section IV. The conclusions are presented in Section V.

## II. Techniques used

This section briefly outlines some techniques that are used to support the proposed *NoMark Method* for copyright protection of digital video content.

### A. Color histogram

The color histogram of an image is a representation of the distribution of colors in that image. It is computed by dividing the image's color space, for example RGB, into a group of $n$ similar colors called *bins* and counting the number of pixels falling into each bin. A color histogram $H$ is a vector $< h_1, h_2, .., h_n >$, in which each bin $h_j$ contains the number pixels of color $j$ in that image. In our approach, two most significant bits of each color channel are used to give a total of $n = 64$ bins in the histogram. For a given image I, the color histogram vector $H_I$ is the compact summary of the image.

### B. Video scene change detection

A video consists of several scenes. Scene change occurs when there is a transition from one scene to another scene. The length of each scene will vary depending upon the number of frames contained with in a scene. Scene change detection is considered a preliminary process in the design of video data management systems used in the content-based search and retrieval of videos [8]–[11]. There are several methods to detect scene changes in a digital video [8], [9], [11], [12]. There are many studies on the survey and comparison of various digital video segmentation and indexing approaches [13], [14]. It has been shown that using a combination of partitioning of successive video frames into equal-sized sub-windows and $\chi^2$ color histogram comparison of corresponding sub-windows yield best results for scene change detection in videos [15].

In the present study, $\chi^2$ comparison of color histogram of consecutive frames is computed by sliding window detector by dividing the window into 4 $(2 \times 2)$ blocks using a step size of half-the-width and half-the-height of the frames. The difference between the color histograms of consecutive frames is computed in RGB color space with 256 bins. Weight for brightness grade change of each color space to calculate the difference among consecutive frames is used to make the scene change detection more robust [12].

### C. Averaged scene image

After the detection of scene changes in a digital video, averaged scene image for each scene is computed by calculating the average color component value for red, green, and blue components for each pixel $(x, y)$ for all the frames in the scene.

### D. Comparison of images

Once the histograms for two images have been computed, a metric for the similarity between the two images can be found by computing the difference of the histogram vectors. Let $H_I$ and $H_{I'}$ are the histograms of the two images $I$ and $I'$. The comparison can be made using $L_2$-distance, sum of squared distances, or $L_1$-distance, sum of absolute value of differences [16]. In our approach, we used the $L_2$-distance, which is given by Equation 1.

$$||H_I - H_I'|| = \sum_{j}^{n} \big(H_I[j] - H_{I'}[j]\big)^2 \quad (1)$$

### E. Visual cryptography based image watermarking

In the year 2000, Ren-Junn Hwang proposed a watermarking method to protect the copyright ownership of a digital image. The method is built up on the concept of visual cryptography and is based on *(2, 2)* visual secret sharing scheme depicted in Table I. According to this method, the owner of an original image, *I*, selects a $h \times n$ black and white image as the watermark pattern *W*. In the embedding process, the owner selects a random number as secret key, *S*, to embed *W* into the image *I*. Let *I* be a $k \times l$ 256 gray-leveled image. Verification information (VI) is generated from *I* based on *(2, 2)*-visual cryptography by defining *W* as the shared image. This verification information becomes first visual cryptographic share of the shared image. The verification information is generated by mapping each pixel in *W* to a pixel at a random location in the image *I*. The color of the pixel in *W* and the MSB value of the corresponding pixel in *I* are used to generate the VI. The process of generating the VI is given below:

- Select a random number as the secret key, S, for the image *I*.

Table I
(2,2) VISUAL THRESHOLD SCHEME

| Pixel in watermark image | Share 1 | Share 2 | Share 1 & 2 superimposed |
|---|---|---|---|
| ■ | ■□ (1,0) | □■ (0,1) | ■■ (1,1) |
| ■ | □■ (0,1) | ■□ (1,0) | ■■ (1,1) |
| □ | ■□ (1,0) | ■□ (1,0) | ■□ (1,0) |
| □ | □■ (0,1) | □■ (0,1) | □■ (0,1) |

Table II
RULES TO ASSIGN VALUES FOR VERIFICATION INFORMATION

| Color of i-th pixel in W | The MSB of $R_i$-th pixel of image I | Assign $(V_{i1}, V_{i2})$ of VI to be |
|---|---|---|
| Black | 1 | (0,1) |
| Black | 0 | (1,0) |
| White | 1 | (1,0) |
| White | 0 | (0,1) |

- Using $S$ as the seed, generate $h \times n$ random numbers over the interval (0,$k \times l$). $i^{th}$ random number is denoted as $R_i$.
- Using Table II, assign $(V_{i1}, V_{i2})$ of $i^{th}$ pair of VI $(V_i)$.
- Construct VI by assembling all the $(V_{i1}, V_{i2})$ pairs.

To verify whether an image $I'$ is a copy of $I$ or the original image $I$ itself, the following process is used to obtain the watermark pattern $W'$. The secret key *S* and *VI* are used in the verification process.

- Use $S$ as the seed to generate $h \times n$ random numbers over the interval (0,$k \times l$). $i^{th}$ random number is denoted as $R_i$.
- Get the most significant bit (MSB), b, of $R_i^{th}$ pixel of image $I'$ to create $i^{th}$ pair of VI' $(V_i')$. If b is 1, then assign $V_i^{'} = (1,0)$; if b is 0, then assign $V_i' = (0,1)$.
- If $V_i'$ is equal to the $i^{th}$ pair of *VI* i.e. $V_i$, assign the color of $i^{th}$ pixel of $W'$ white or else assign it black.
- If $W'$ is recognized as $W$ by the human visual system, then it can be inferred that $I'$ is same as $I$ or a copy of it.

Figure 1. Watermark image.

### F. Encryption, digital signature and digital timestamp

With the introduction of public-key cryptosystems and digital signature by Rivest, Shamir and Adleman in 1978 [17], verification of authenticity and integrity of an electronic document or a file became a reality. Digital signature along with digital timestamp is a proof of authenticity, integrity, and time of creation of electronic data. To secure the data from unauthorized access and cyber theft, the data shall be encrypted after digital signature and timestamp. For encryption, the owner of the video can use his or her own public key. While submitting it to an agency for verification at the time of any dispute over copyright infringement, the owner can decrypt with his or her private key and submit to designated agency or person after encrypting with the public key of that agency or person.

## III. PROPOSED NOMARK METHOD

Copyright infringement of a digital video can happen in many ways, some of which are, falsely claiming ownership of a video, illegally embedding scenes from other videos, claiming ownership of a video after modifications such as frame dropping, frame swapping, frame averaging, video fragmentation, scene dropping, and scene swapping or combinations of these modifications. The watermarking method presented in our previously published work [18] is capable of detecting false copyright claims after attacks such as frame dropping, frame swapping, and frame averaging. In other copyright infringement cases, the previous method is either not capable of detecting the watermark pattern accurately or efficiently if there is a scene dropping or the number of scenes in the original video and the suspect video are different. In this section, we present a robust, reliable, and efficient method called *NoMark Method* for the copyright protection of videos and scenes contained therein.

One of the two shares of *(2, 2)* visual secret sharing scheme for a scene in the video to be protected is created using a secret key, watermark pattern, and averaged scene image while the second share is created using the same secret key and averaged scene image of the video to be verified during the *NoMark* verification process. Overlapping these two shares during the verification process results in the retrieved watermark pattern which will be same as the original watermark pattern only if the averaged scene images and the secret key used in verification process are same as those used in the protection process.

### A. NoMark protection process

A sample video named *Bless Your Pet* downloaded from *http://www.washingtonpost.com/* is used as the original video (*F*) and the watermark pattern *W* given in Figure 1 are used to implement and demonstrate the method presented in this section. The method of *NoMark* Protection consists of the following steps:

i). Apply the scene change detection algorithm given in Section II-B on the video $F$ to be protected, to compute scene start point information vector which gives location of the key frame at which new scene starts.

ii). Compute averaged scene image corresponding to each scene in the video using scene start point information vector. Averaged scene image is computed by averaging the color component values of corresponding pixels for all frames in the scene.

iii). Compute the color histogram for each averaged scene image using algorithm described in Section II-A. Two most significant bits of each color channel are used for a total of $n = 64$ bins in the histogram. For a given image *I*, the color histogram information vector $H_I$ is the compact summary of the image. Store all the computed color histograms for future verification process.

iv). Each averaged scene image is converted to a grayscale image and it's *VI* is computed using method described in Section II-E. The number of verification information vectors to be constructed is equal to the number of scenes in the video to be protected. The VI vector is one of the two shares generated from the watermark pattern *W*, secret key *S* and averaged scene image *I* using $(2, 2)$-visual threshold scheme. The second share will be computed during the verification process. As the random sequence is governed by the secret key, it is difficult for anyone else other than the copyright owner of the video to detect the pixels concerning the watermark pattern.

v). Digitally sign and timestamp secret key *S* and each VI to obtain $VI_{sd}$ and securely store them encrypted for future verification in case of any copyright infringement. Each computed visual cryptographic share *VI* corresponding to a scene in the protected video is mapped with the histogram information $H_I$ corresponding to that scene's averaged image.

The above protection method is depicted as flow chart in Figure 2.

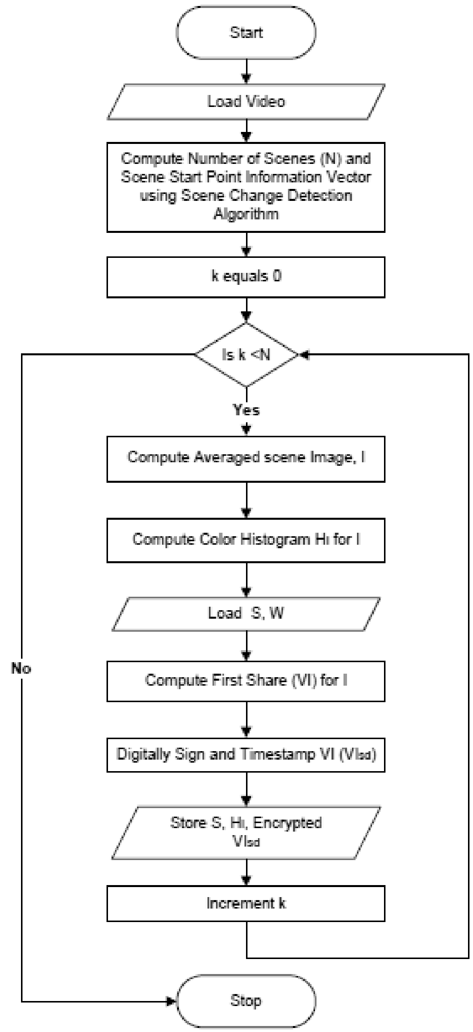


Figure 2. Flowchart for NoMark Protection method.

### B. *NoMark verification process*

When there is a suspicion of copyright infringement, the owner of the original video *F* needs to submit the following to a verification authority in a secure manner:

- The secret key *S* used to generate random numbers for the purpose of computing *VI* for each averaged scene image. Instead of *S*, the set of random numbers generated using *S* can also be submitted.
- Computed histograms corresponding to each protected scene.
- Digitally signed and timestamped verification information vectors of all the *NoMark* protected scenes.
- The watermark pattern.
- Digital certificate.

If the copyright owner of video *F* suspects that another video $F'$ is a copy of *F* or contains scenes from *F*, then the following process is used for the purpose of verification of the copyright ownership and any infringement:

i). Decrypt each submitted $VI_{sd}$ and obtain *VI* after verifying the digital signature and timestamp using the public key contained in the submitted digital certificate. If the digital signature verification process fails for any $VI_{sd}$, then it is discarded for extraction of watermark pattern, as it is tampered. The corresponding Histogram Information Vector can not be used to find the best match of the averaged scene image as the share (*VI*) is altered.

ii). If the digital signature verification fails for all the submitted $VI_{sd}$, then any claim of infringement by $F'$ on the copyright of $F$ is rejected.

Subsequent steps are carried out only if digital signature verification for all or some of the $VI_{sd}$ are successful.

iii). Detect scene changes in the video $F'$ and compute scene start point information vector using the method given in Section II-B.

iv). Averaged scene image *I'* corresponding to each scene in the video is computed. Scene start point information vector is used to get the boundaries of scene and then simple averaging is done on the corresponding pixels for all the frames within the boundary.

v). Compute the color histogram information vector ($H_{I'}$) for each averaged scene image using two most significant bits of each color channel for a total of $n = 64$ bins in the histogram.

vi). Compute the second cryptographic share *VI'* using *I'* computed above and submitted *S* as described in Section II-E.

vii). Compare the histogram ($H_{I'}$) computed in Step (v) with the set of histograms submitted by the claimant. Evaluate the best possible match from the set using the sum of squared differences ($L_2$-distance). The most similar histogram would be the one minimizing the equation 1.

The most similar histogram match is performed so that the correct combination of shares are overlapped to retrieve the watermark pattern. The histogram match algorithm will not consider the histogram information vectors corresponding to the verification information vectors for which the digital signature verification process failed in Step (i).

viii). Overlap the second share which is *VI'* vector on to the first share *VI* vector corresponding to the histogram obtained in the Step (vii) to retrieve the watermark pattern using process described in Section II-E. Save the retrieved watermark pattern *W'* for each averaged scene image.

ix). To analyze numerically the similarity between original watermark pattern *W* and retrieve watermark pattern *W'*, Root Mean Square (RMS) value of pixels as a measure of noise is computed using Equation 2. The difference between the RMS value of *W'* and *W* results in the RMS value of noise, as the noise in a binary image is the increase in the density of black or white pixel. Other basic correlation measures can also be used to benchmark NoMark method using appropriate threshold selected using probability of false alarm.

x). The similarity between retrieved watermark pattern and original watermark pattern is also verified by visual inspection.

xi). If the retrieved watermark pattern and the original watermark pattern are visually similar and the RMS energy of noise is below certain threshold, then it can be inferred that there is a copyright infringement.

$$RMS\ energy = 10 \log \sqrt{\frac{1}{M \times N} \Big( \sum_{i=1}^{M} \sum_{j=1}^{N} I^2(i,j) \Big)}\ dB \tag{2}$$

The above verification process is depicted in flow chart given in Figure 3.

## IV. Simulation results and discussions

For the simulations, two video files *Bless Your Pet* (referred to as *F1*) and *Stocking up for the 'storm of the decade'* (referred to as *F2*) both downloaded from *www.washington-post.com* [19] are used after ensuring same format (avi) and resolution. *F1* consists of a total of 2964 frames and 22 scenes while *F2* consists of a total of 1740 frames and 21 scenes. To simulate detection of copyright infringement, scene 17 from *F1* is inserted into *F2*. Let the modified video be called $F2'$.

The following two test cases are used to demonstrate the effectiveness of the NoMark Protection method in establishing any copyright infringement. *F1* is watermarked using the method described in Section III-A by the copyright owner.

- The copyright owner of *F1* suspects that *F2* is an unauthorized copy of *F1*.
- The copyright owner of *F1* suspects that $F2'$ is infringing on the copyright of *F1* by unauthorized inclusion of a scene from *F1*.

In order to verify the claims of the copyright owner of *F1* as per two test cases above, the NoMark Verification Process described in Section III-B is used first on *F2* and then on $F2'$ using the data submitted by the owner of *F1* as given in the same Section. The results are given below:

1). To simulate the first test case, NoMark Verification Process is applied on *F2*. Since the videos *F1* and *F2* are different, none of the computed color histogram of *F1* will be equal to that of any scene in *F2*. Using the verification process given in Section III-B for each scene in *F2*, the best matching scene from *F1* is selected using most similar histogram test. The corresponding VI is used to extract the watermark pattern and visually compared with the original watermark pattern used in the protection process given in Figure 1. For none of the scene, the extracted watermark pattern of scenes in *F2* and original watermark pattern used to protect scenes of *F1* are visually identical. The results are illustrated in Figure 4 for four sample scenes of *F2*.

2). To simulate the second test case given above, scene 17 from *F1* is inserted after scene 10 in video *F2*. It can be inserted at any arbitrary location. The modified video is referred to as $F2'$. When the verification process given in Section III-B is applied on video $F2'$, the histogram

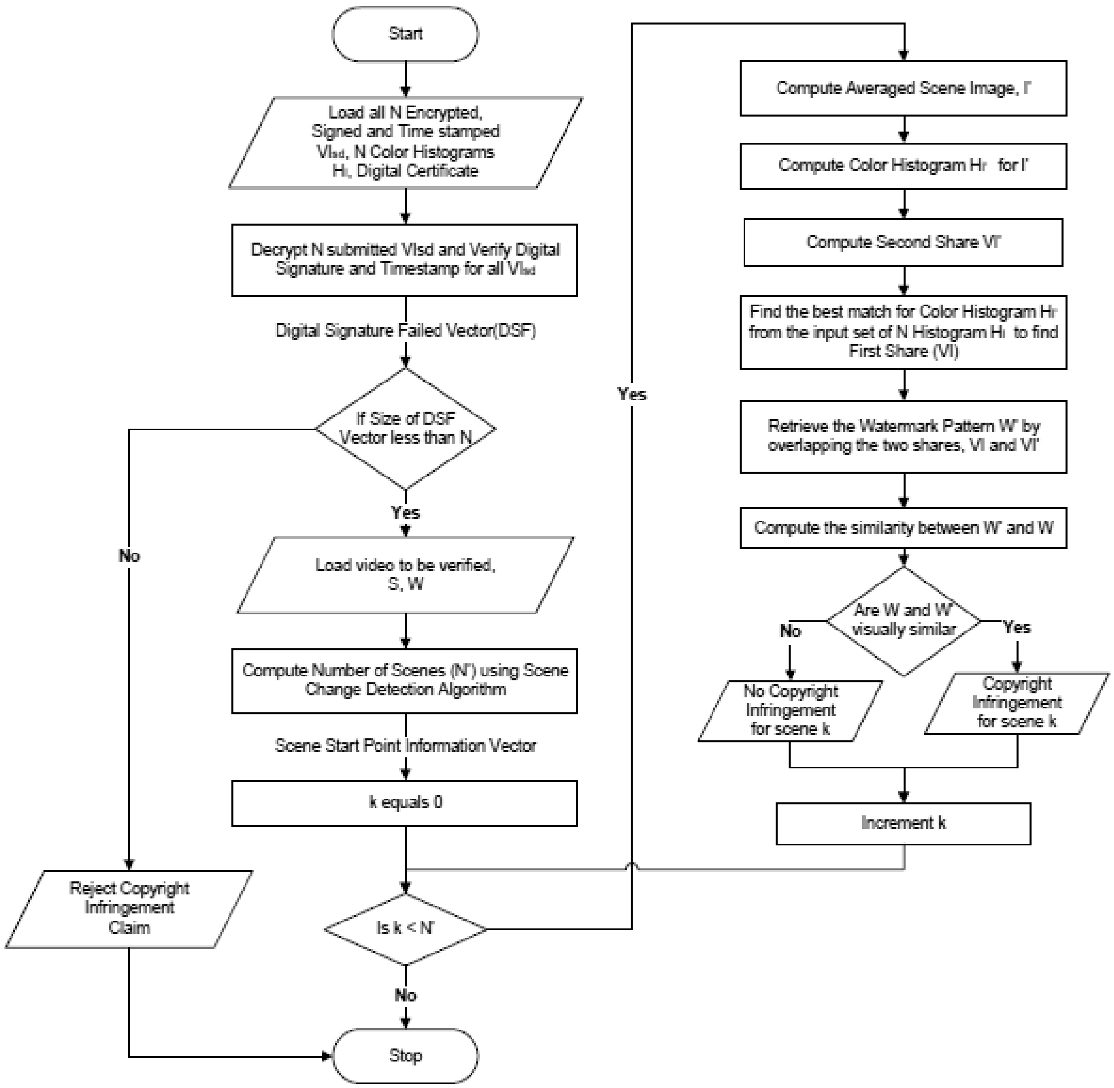


Figure 3. Flowchart for NoMark Verification method.

of scene 17 of *F1* matches with that of scene 11 of $F2'$. Watermark pattern of scene 11 of $F2'$ is extracted by overlapping the shares corresponding to scene 11 of $F2'$ and scene 17 of *F1* and is visually compared with the original watermark pattern as given in Figure 1. Scene start image, scene averaged image and extracted watermark pattern using corresponding VI for scene 17 of *F1* are given in column $(i)$ of Figure 5. Scene start image, scene averaged image and extracted watermark pattern using VI of scene 17 of *F1* for scene 11 of $F2'$ are given in column $(ii)$ of Figure 5. We can see that the extracted watermark pattern visually matches with the original watermark.

3). Tests were also conducted by inserting scene 17 of *F1* after scene 10 in *F2* after dropping every alternate frames of scene 17. Scene start image, scene averaged image and extracted watermark pattern using VI of scene 17 of *F1* for scene 11 of $F2'$, which is basically scene 17 of *F1* with alternate frames dropped, are given in column $(iii)$ of Figure 5. The extracted watermark pattern again visually matches with the original watermark. As can be seen from column $(iv)$ of Figure 5, the extracted watermark pattern visually matches with the original watermark pattern even when last 50% of the frames of scene 17 of *F1* are dropped before inserting into *F2*.

4). The time taken to retrieve the watermark pattern by

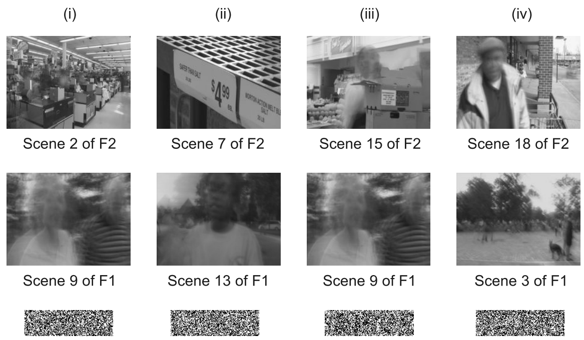


Figure 4. Simulation results for using VIs of scenes in *F1* on scenes in *F2* to extract watermark pattern. Averaged scene images of scenes 2, 7, 15, and 18 of *F2* are given in top row of images. Middle row gives averaged scene images of scenes in *F1* with best matching histograms. Bottom row gives watermark patterns extracted from scenes in $F2$ using VI of scenes in F1 with best matching histogram.

Table III
RMS ENERGY OF NOISE IN RETRIEVED WATERMARK PATTERN

| Test Case | RMS energy of noise (dB) |
|---|---|
| Frames are randomly dropped | 0.0924 |
| Every fourth frame dropped | 0.1450 |
| Every second frame dropped | 0.1483 |
| Last 25% of scene dropped | 0.1514 |
| Last 50% of scene dropped | 0.2014 |
| Shares from different scenes overlapped | 0.9653 |

overlapping the shares is significantly improved by identifying the matching share using most similar histogram comparison instead of overlapping the shares of all the scenes of *F1* with the share of each scene of *F2* one by one in a brute force manner. With this method, the time taken to retrieve the watermark pattern for a scene in *F2* is only 6.3% of the time taken in brute force manner.

5). The RMS energy of noise in the retrieved watermark pattern as compared to the original watermark pattern for scene 11 of the video $F2'$ is given in Table III. From the table, it is clear that the RMS energy of noise increases as the number of frames dropped from the scene 17 of $F1$ increases and the noise is highest when first share from a different scene is overlapped.

Time taken by various sub-processes of the NoMark verification process for video *F1* is given in Figure 6. It is evident that only 1% of time is taken for retrieval of watermark pattern, almost 72% of time is taken for scene change detection and 27% of time is taken by computation of averaged scene image and color histogram. Time complexity of *NoMark* protection and verification processes can significantly improve by reducing time taken for scene change detection and computation of averaged scene image.

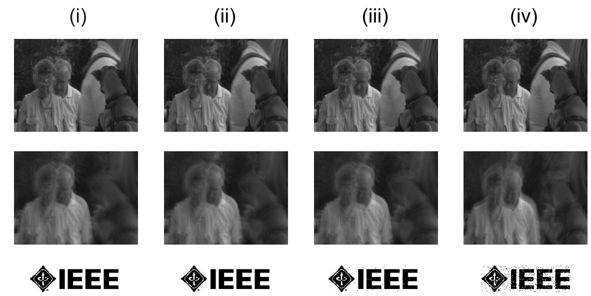


Figure 5. Simulation results for infringement detection. (i). For scene 17 in F1 - Scene start frame (top), Scene averaged image (middle), and Retrieved watermark pattern (bottom) with 0% frame drop. (ii). For scene 17 of F1 inserted in F2 - Scene start frame (top), Scene averaged image (middle), and Retrieved watermark pattern (bottom) with 0% frame drop. (iii). For scene 17 of F1 inserted in F2 after 50% frame drop (alternate frames dropped) - Scene start frame (top), Scene averaged image (middle), and Retrieved watermark pattern (bottom). (iv). For scene 17 of F1 inserted in F2 after 50% frame drop (last 50% frames dropped) - Scene start frame (top), Scene averaged image (middle), and retrieved watermark pattern (bottom).

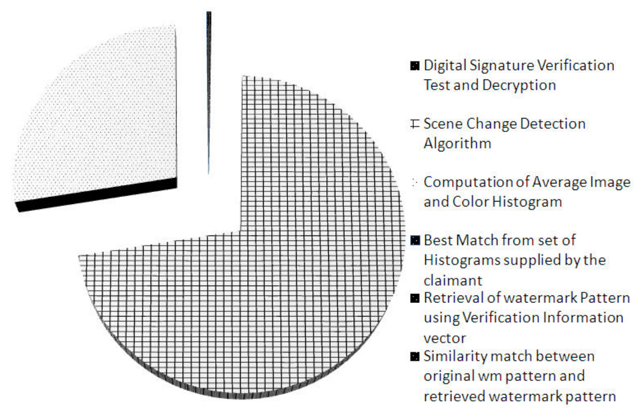


Figure 6. Time taken by various sub-processes of NoMark Verification method.

## A. Further improvements

Work on further improvements on the method presented in this paper are in progress. Some of the improvements are listed below:

- The method needs improvements to make it robust against rescaling, cropping, and rotation.
- The method is not yet tested to compare video recordings of same scenario of a football match, from two different angles.

## V. CONCLUSIONS

The NoMark Method presented in this paper is based on Visual Cryptography and can be used for the copyright protection of entire digital video or individual scenes contained therein. Some techniques such as scene change detection, computation of averaged scene image, computation and comparison of histogram of images are used. First visual cryptographic share corresponding to each scene is computed using averaged scene image, a secret key and a watermark pattern. Digital Signature and timestamp are used to verify the authenticity and integrity of this share. Confidentiality of the signed timestamped share is protected by encryption before storage or transmission. During the verification process, second cryptographic share is computed for each scene of the video to be verified using averaged scene image and the submitted secret key. Most similar histogram match is performed to identify the correct combination of visual cryptographic shares that are to be overlapped to retrieve watermark pattern. Retrieved watermark pattern will be similar to original watermark pattern only if the averaged scene image and secret key used to create corresponding shares are same in both the NoMark protection and verification processes.

The proposed method is efficient against various watermark attacks like frame averaging, frame swapping, frame dropping, interpolation and statistical analysis, collusion attacks, scene dropping, video fragmentation, unauthorized inclusion of scenes in other videos, lossy video compression, sharpening, blurring, up to 10% variations in lightening, contrast changes, distortion, noising, jittering. Rather than watermarking all the scenes, scene may also be selected in an intelligent manner for watermarking.

## REFERENCES


[1] Nielsen, "Television, Internet and Mobile Usage in the U.S.: Three Screen Report 4th Quarter 2009," 2009. [Online]. Available: http://en-us.nielsen.com/main/insights/nielsen_a2m2_three/

[2] J. Kennedy, "DIGITAL MUSIC REPORT 2009: New Business Models for a Changing Environment," IFPI, Tech. Rep., Jan. 2009.

[3] M. P. A. of America, "Worldwide Study of Losses to the Film Industry & International Economies due to Piracy; Pirate Profiles," May 2006. [Online]. Available: http://www.iipa.com/copyright_us_economy.html

[4] C. Ray and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP Journal on Applied Signal Processing*, pp. 613–621, 2006.

[5] R. Manjunatha Prasad and S. Koliwad, "A comprehensive survey of contemporary researches in watermarking for copyright protection of digital images," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 4, pp. 91–107, Apr. 2009.

[6] M. Naor and A. Shamir, "Visual cryptography," in *EUROCRYPT*, 1994, pp. 1–12.

[7] R.-J. Hwang, "A digital image copyright protection scheme based on visual cryptography," *Tamkang Journal of Science and Engineering*, vol. 3, no. 2, pp. 97–106, 2000.

[8] A. Hampapur, T. Weymouth, and R. Jain, "Digital video segmentation," in *MULTIMEDIA '94: Proceedings of the second ACM international conference on Multimedia*. New York, NY, USA: ACM, 1994, pp. 357–364.

[9] C. F. Lam and M.-C. Lee, "Video segmentation using color difference histogram," in *MINAR '98: Proceedings of the IAPR International Workshop on Multimedia Information Analysis and Retrieval*. London, UK: Springer-Verlag, 1998, pp. 159–174.

[10] C.-W. Chang and S.-Y. Lee, "Video content representation, indexing, and matching in video information systems," *Journal of Visual Communication and Image Representation*, vol. 8, no. 2, pp. 107 – 120, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/B6WMK-45KKSGK-2/2/a9e7ac7050d7d12aeb0241b92efb8ca2

[11] R. Zabih, J. Miller, and K. Mai, "A feature-based algorithm for detecting and classifying scene breaks," in *MULTIMEDIA '95: Proceedings of the third ACM international conference on Multimedia*. New York, NY, USA: ACM, 1995, pp. 189–200.

[12] P. Adhikari, N. Gargote, J. Digge, and B. Hogade, "Abrupt scene change detection," *World Academy of Science, Engineering and Technology*, vol. 42, pp. 711–716, 2008.

[13] M. H. Kolekar and S. Sengupta, "Video shot boundary detection: A comparative study of three popular approaches."

[14] G. Ahanger and T. D. C. Little, "A survey of technologies for parsing and indexing digital video," *Journal of visual Communication and image representation*, vol. 7, pp. 28–43, 1996.

[15] H. Jiang, A. S. Helal, A. K. Elmagarmid, and A. Joshi, "Scene change detection for video database management systems - a survey," Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, Tech. Rep. CSD-TR 96-058, Oct. 1996.

[16] G. Pass, R. Zabih, and J. Miller, "Comparing images using color coherence vectors," in *MULTIMEDIA '96: Proceedings of the Fourth ACM International Conference on Multimedia*. New York, NY, USA: ACM, 1996, pp. 65–73.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[18] A. Vashistha, R. Nallusamy, and S. Paul, "Watermarking video content using visual cryptography and scene averaged image," in *International Workshop on Content Protection and Forensics (CPAF 2010), In Conjunction with IEEE International Conference on Multimedia and Expo (ICME 2010), July 19 - 23, 2010, Singapore*, 2010.

[19] washingtonpost.com, "News and documentary videos from the washington post." [Online]. Available: http://cdn.washingtonpost.com/