Digital Fingerprinting for Piracy Control

Neha Sharma
M.Tech. Student
Department of Computer Science
Punjabi University, Patiala

Sukhjeet Kaur Ranade
Associate Professor
Department of Computer Science
Punjabi University, Patiala

ABSTRACT
Aiming at the secure, robust and perceptually invisible data hiding goal, a Discrete Cosine Transform (DCT) based blind video watermarking algorithm which is robust against collusion attack is proposed in this paper. This research work embeds the binary code acting as a digital fingerprint in the video frame that uniquely recognizes the authenticated user. The fingerprints are designed in the DCT domain that resist collusion and controls piracy. The confidentiality of the original frame is achieved by embedding watermark logo at the random blocks in the successive frames of the video. This is done by using Pseudo Random Number (PRN) generator whose seed value generated by a permutation vector acts as a secret key (K). During the extraction of watermark information, the same permutation vector is used to regenerate the secret key as well as the selection of the embedding blocks. This achieves the piracy control in digital fingerprinting mechanism as none of unauthorized users can tamper the original content. The experimental results show that the proposed scheme is robust against the collusion attack.

General Terms
Digital fingerprinting, Collusion attack.

Keywords
DCT, Collusion attack, Pseudo random number, Watermark embedding, Robustness.

1. INTRODUCTION
Digital Fingerprinting is a technology which includes the embedding of additional hidden data into multimedia content. These data are known as fingerprints and each fingerprint recognizes one individual user of the system. These fingerprints can facilitate to identify the culprits who use their content for illegal purposes. Sometimes, a group of rogue users mount attack against these fingerprints collectively, known as multi-user collusion attacks. There is a need to maintain security of owner's content from this type of attacks. To protect the content from grabbers, design the fingerprints in a way that it would become hard to detect and destroy these embedded fingerprints.

During the development of a video watermarking algorithm, the researchers must be concerned of two issues: visual imperceptibility and robustness. Visual imperceptibility means perceptual transparency, that is, the quality of the video frames is not visually affected even if the watermark is embedded into the frame. Robustness means video frames withstand malicious attacks while extracting watermark and a successful extraction from the frame takes place.

Digital Fingerprinting is evolving, as it works as a platform for detecting rogue users or pirates and enable owners to monitor their content authenticity and reduce instances for copyright violation.

2. DISCRETE COSINE TRANSFORM
Discrete Cosine Transform (DCT) is one of the transform domain techniques. This mathematical transformation converts the pixels in such a way as to convey the impact of "spreading" location of the pixel values over part of the image. The DCT transforms a signal from an image representation into a frequency representation, by grouping pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT [4]. It eliminates all higher frequency DCT coefficients thus reduces the size of equations.

2.1 The One Dimension DCT
The 1-D DCT is defined as:

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right], \quad (1)$$

For $u = 0, 1, 2 \ldots\ldots N-1$

To reconstruct the modified image, inverse DCT is applied. The inverse transformation is defined as:

$$f(x) = \sum_{u=0}^{N-1} \alpha(u) C(u) \cos\left[\frac{\pi(2x+1)u}{2N}\right], \quad (2)$$

For $x = 0, 1, 2 \ldots\ldots N-1$

where,

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}}, & \text{for } u = 0 \\ \sqrt{\frac{2}{N}}, & \text{for } u \neq 0 \end{cases} \quad (3)$$

Thus, the first transform coefficient is the average value of the sample sequence. In this literature, the value is termed as DC Coefficient. All other transform coefficients are referred to as AC Coefficients [3].

2.2 The Two Dimension DCT
The 2-D DCT is the extension of 1-D DCT. It is defined as:

$$C(u,v) = = \alpha(u)\alpha(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (4)$$

For $u, v = 0, 1, 2 \ldots\ldots N-1$ and $\alpha(u)$ and $\alpha(v)$ are given in equation (3).

The inverse transformation is defined as:

$$f(x,y) = = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u)\alpha(v) C(u,v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (5)$$

For $x, y = 0, 1, 2 \ldots\ldots N-1$

This technique achieves de-correlation of the image content and acquires decrease in entropy of the image content. Thus, separate components are encoded and modified using DCT transform coefficients.

3. COLLUSION ATTACK

It must be supposed that pirates are familiar of the existence of fingerprints in their copies and that they would carry out several attacks intended to destroy the fingerprints. The greatest hazard to the mass multimedia distribution is organized groups of pirates who analyse the fingerprinted copies available to them. Finally produces a pirated copy which is free of fingerprints or holds a damaged fingerprint that does not recognizes the real pirates. Such attacks are known as collusion attacks. Thus, fingerprinting methods must be designed to provide resilience to such attacks [5].

In the scheme, a binary code which uniquely identifies a customer of the multimedia content is embedded into the document prior to its distribution. This binary code acts as a digital fingerprint for that authenticated customer. Sometimes, a single colluder or a group of colluders collectively grab the original content copy and generate a pirated copy having destroyed fingerprints. The scheme must be designed in a way that not any unauthorized user can tamper the original content. These fingerprints are later on extracted to trace the rogue users who mounted attack on the multimedia data.

4. RELATED WORK

Comprehensive literature survey is done to identify the problems in previous research work. Many researchers proposed several image and video watermarking algorithms in the past few years. However, the goal is to achieve perceptual transparency and robustness against various attacks while implementing the algorithm.

Boneh and Shaw [1] have discussed methods for assigning code words for the purpose of fingerprinting digital data. They have assumed that secure marks could be embedded in the fingerprinted data. This marking would allow a distributor to detect any unauthorized copy and traced it back to the user. In addition, they discussed the methods for distributing fingerprinted data.

Barni M. et al., [2] have presented a new watermarking algorithm for digital images that operated in frequency domain and embedded a pseudo random sequence of real numbers in a selected set of DCT coefficients. This method provided robustness against various signal processing techniques.

Dzwonkowski M. et al., [5] have demonstrated a potential application for the error patterns which occurred after the decryption in digital fingerprinting. They offered gaining the possibility of pirate tracing in case of collusion attack while maintaining confidentiality through encryption of the transmitted data would allow us to successfully extend the security boundaries offered by multimedia distribution systems.

Manaf A. et al., [6] have proposed a frame-by-frame blind watermarking method to enhance copyright protection of the digital videos. They used a combination of Block Truncation Coding (BTC), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) methods to preserve quality as well as robustness against collusion attack as each frame received a unique watermark.

Karmakar A. et al., [7] have proposed a DCT based blind video watermarking algorithm which was perceptually invisible and robust against rotation and collusion attack. Zernike moments were calculated to predict the rotation angle of the video at the time of extraction of watermark bits. To make scheme robust against collusion attack, embedding blocks of successive frames in the video varied.

5. PROPOSED SCHEME

Our approach is a Discrete Cosine Transform (DCT) based blind video watermarking which is robust against the collusion attack. The confidentiality of the original frame is achieved by embedding watermark at the random blocks in the successive frames of the video. A Pseudo Random Number (PRN) generator and a permutation vector are used to attain the goal. The scheme is carried out in the following three phases:

- Watermark Embedding
- Watermark Extraction
- Watermark Authentication

5.1 Watermark Embedding

In this phase, watermark is embedded in the selected frame of video. A binary logo is taken as a watermark logo whose every bit is either '0' or '1' that acts as a digital fingerprint for that frame. Firstly, RGB frame is converted into HSV (hue, saturation, value-brightness) frame as RGB has the most correlated components that are not suitable for embedding watermark in any of the components. On the other hand, HSV allows segmentation of the achromatic part from the chromatic part that permits us to embed the watermark in the luminance parts of the video frame.

The embedding of the watermark logo in the selected frame of the host video is carried out in the following steps:

Step 1: Extract the frames from host video one by one.
Step 2: Convert the color model of the extracted frame from RGB to HSV according to equations (6), (7) and (8).

$R' = R/255 \quad G' = G/255 \quad B' = B/255$
$C_{max} = max\,(R', G', B')$
$C_{min} = min\,(R', G', B')$
$\Delta = C_{max} - C_{min}$

Hue Calculation:

$$H = \begin{cases} 0° & \Delta = 0 \\ 60° \times \left(\frac{G`-B`}{\Delta} mod 6\right), & Cmax = R' \\ 60° \times \left(\frac{B`-R`}{\Delta} + 2\right), & Cmax = G' \\ 60° \times \left(\frac{R`-G`}{\Delta} + 4\right), & Cmax = B' \end{cases} \quad (6)$$

Saturation Calculation:

$$S = \begin{cases} 0 & , Cmax = 0 \\ \frac{\Delta}{Cmax} & , Cmax \neq 0 \end{cases} \quad (7)$$

Value Calculation:

$$V = C_{max} \quad (8)$$

where H represents hue, S represents saturation and V represents value of brightness and Δ represents chromaticity. C_{max} and C_{min} are maximum and minimum of the RGB components respectively.

Step 3: A square block of size (M × M) is selected in each luminance component's middle which is considered as the target embedding area. The block (M × M) is divided into non-overlapping sub-blocks of size (8×8). These blocks in

which data is embedded are chosen pseudo randomly (key dependent). This makes the scheme secured.

Step 4: Then 'N' number of distinct blocks of size (8×8) where the watermark logo is to be embedded are chosen pseudo randomly.

Step 5: Apply 2D DCT on each selected blocks of size (8×8).

Step 6: Select 'n' number of AC components pseudo randomly for each DCT block (8×8). These 'n' number of AC coefficients of a block (8×8) are used for embedding one bit of watermark. The same mechanism of Step-4 is used for secret key management of PRN generator. The modification of AC components is done according to the rule as follows:

if $(W(k) == 1)$
do {
if $(\text{mod } (A(r,s),d) \leq a)$
$A_w(r,s) = A(r,s) - \text{mod } (A(r,r),d) - a$
else
$A_w(r,s) = A(r,s) - \text{mod } (A(r,s),d) + c$
endif
} until 'n' number of AC coefficients are considered.
elseif $(W(k) == 0)$
do {
if $(\text{mod } (A(r,s),d) \geq c)$
$A_w(r,s) = A(r,s) - \text{mod } (A(r,r),d) + e$
else
$A_w(r,s) = A(r,s) - \text{mod } (A(r,s),d) + a$
endif
} until 'n' number of AC coefficients are considered.
endif

where, $W(k)$ is the watermark bit to be embedded, $A(r,s)$ is the original AC component, $A_w(r,s)$ is the watermarked AC components. Here, a, b, c, d and e are the embedding strength and considered as the global constants. The relation between these global constants is $b = 2a$, $c = 3a$, $d = 4a$ and $e = 5a$. The values are chosen based on the experimentation, such that, the robustness and fidelity of the watermarked video is within an acceptable range. The function $\text{mod } (A(r,s),d)$ is the remainder of $A(r,s)$ and d.

Step 7: Repeat Steps 1-6 until all the video frames are considered.

Step 8: Convert HSV to RGB color model according to equations (9) and (10) and merge all frames to construct the watermarked video.

When $0 \leq H < 360, 0 \leq S \leq 1$ and $0 \leq V \leq 1$:

$$C = V \times S$$

$$X = C \times (1 - |(H / 60°) \bmod 2 - 1|)$$

$$m = V - C$$

$$(R', G', B') = \begin{cases} (C, X, 0) & , 0° \leq H < 60° \\ (X, C, 0) & , 60° \leq H < 120° \\ (0, C, X) & , 120° \leq H < 180° \\ (0, X, C) & , 180° \leq H < 240° \\ (X, 0, C) & , 240° \leq H < 300° \\ (C, 0, X) & , 300° \leq H < 360° \end{cases} \quad (9)$$

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} (R' + m) \times 255 \\ (G' + m) \times 255 \\ (B' + m) \times 255 \end{pmatrix} \quad (10)$$

where R represents red color, G represents green color and B represents blue color of RGB color model. X and m are the computed values used while conversion. H represents hue, S represents saturation and V represents value of brightness in HSV color model.

5.2 Watermark Extraction

It is the reverse part of the embedding phase.

- As the name blind video watermarking, "blind" means that the scheme does not require the original data and the embedded watermark while extraction of the watermark logo.
- However, to determine the position of the embedding block, the extraction algorithm has to know only about the seed value of the random number generator which it used earlier during the embedding of the watermark bits.

The watermark extraction is explained as follows:

Step 1: Frames are extracted from the watermarked video one by one.
Step 2: Change the color model of the extracted frame from RGB to HSV according to equations (6), (7) and (8).
Step 3: A square $(M \times M)$ sized block is chosen from the luminance's component middle which was used as the embedding area. Then the block is divided into non-overlapping (8×8) sized sub-blocks.
Step 4: Same Pseudo Random Number (PRN) generator is used to choose the same N number of (8×8) sized blocks, where the watermark bits were embedded.
Step 5: Apply 2D DCT on each selected blocks of size (8×8).
Step 6: Choose the same *'n'* number of AC components pseudo randomly which was modified during the embedding process and the watermark bit is detected according to the rule as follows:
do
if $(\text{mod } (A_w(r,s),d) > b)$
$W_{extract}(b) = 1$
else
$W_{extract}(b) = 0$
endif
} until 'n' number of AC coefficients are considered.
where $1 \leq b \leq n$ and $W_{extract}(b)$ are the extracted watermark bit and $A_w(r,s)$ is the watermarked AC components. Then final decision of extracted watermark bit $W(k)$ from a block of size (8×8) is taken depending on the maximum occurrence of 1 or 0 in $W_{extract}(b)$.
Step 7: Repeat Steps 2-6 until all watermark bits are extracted.

5.2 Watermark Authentication

This phase is achieved by comparing the extracted watermark with the original watermark.

- We quantify the visual quality of the extracted watermark, by calculating Normalized Cross Correlation (NCC) between the original watermark and the extracted watermark. Thus, it helps us to

identify if any tampering or manipulation is done to the watermarked frame.

- If any unauthorized user extracts watermark with a fake key, the extracted logo looks like noise. Since our scheme is sensitive to key and hence secured.

6. RESULTS AND DISCUSSIONS

In this paper, the proposed scheme of watermark embedding and watermark extraction algorithms in MATLAB is implemented. The simulation is carried out on six standard videos. In this scenario, we have taken 250 frames of size (512×512) of each host video. A binary logo embedded into the video frames is of size (50×25). The square luminance block taken is of size (176×176), where this watermark logo is embedded. The value of N as mentioned in Step 4 of the embedding algorithm is chosen according to the size of the binary logo. The value of global constant (a) mentioned in Step 6 of the embedding algorithm is taken as 13.

The proposed technique is compared against one of the existing technique mentioned in the literature for making a comparative analysis. The existing technique had worked on YC_bC_r (luminance, chrominance-blue, chrominance-red) color model. We have improved the quality index metrics by conducting the work on HSV (hue, saturation, value-brightness) color model. It is advantageous in HSV color model to separate color from intensity component for the real time applications.

Table 1 is showing the various videos used for experimentation in which different watermarks are embedded. All the video frames are of same extension on which the proposed scheme as well as the existing scheme is implemented.

Table 1. Video frames taken for experimental analysis

Video name	Extension	Watermark	Extension
Aeroplane take-off	.wmv	Google	.jpeg
Athletics	.wmv	Logo1	.jpeg
Wildlife	.wmv	Logo2	.jpeg
Space shuttle	.wmv	Google	.jpeg
Australian grand	.wmv	Logo3	.jpeg
Cycling	.wmv	Logo4	.jpeg

6.1 Experimental Results

Fig. 1: Original frame (512×512) of video 'Aeroplane Takeoff'

Figure 1 shows the original frame taken from host video namely 'Aeroplane takeoff.wmv'. The embedding algorithm is implemented on the video frame (512×512).

Fig. 2: Watermarked video frame (512×512)

Figure 2 has shown the watermarked video frame of proposed algoritm. Comparing the watermarked frame with the original frame reveals no difference visually. So, the proposed algoritm achieves visual imperceptibility.

Fig. 3: Original watermark image (50×25)

Figure 3 shows the watermark logo of size (50×25) which is embedded into the video frame.

Fig. 4: Extracted watermark image (50×25) from watermarked video frame with NCC = 1

Figure 4 has shown the extracted watermark using proposed algoritm. Comparing the extracted watermark with the original watermark reveals no difference as it does not looks noisy. So, quality in the proposed algoritm is preserved.

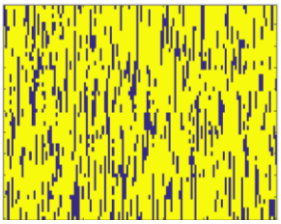

Fig. 5: Extracted watermark image using fake key

Figure 5 has shown the extracted watermark of proposed algorithm using fake key. By comparing the extracted watermark with the original watermark, it is observed that a noisy information is extracted by any unauthorized user. So, the proposed algorithm is robust against collusion attack hence secured.

6.2 Performance Evaluation

Different host videos are used for the purpose of experimentation. The results are analysed using various parameters like Peak to Signal Noise Ratio (PSNR), Mean Structure Similarity Index (MSSIM), and Normalized Cross Correlation (NCC). The experimental results show the better performance of the proposed scheme over the existing scheme.

Table 2. Comparison analysis on basis of PSNR parameter

Video name from which frame has been tested	Existing method	Proposed method
Aeroplane take-off	40.2636	42.6419
Athletics	39.5377	43.0138
Wildlife	39.9415	42.1501
Space shuttle	39.8269	42.4336
Australian grand	39.9541	43.7647
Cycling	39.6537	42.3893

Table 2 has shown the proposed method outperforms over the existing method in terms of parameter PSNR (dB).

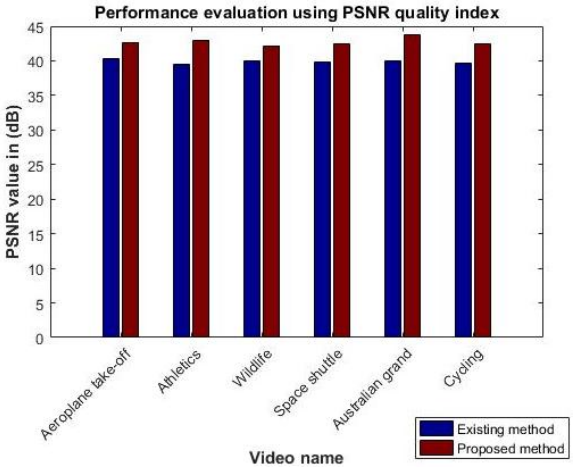

Fig. 6: Graph representing PSNR (in dB) value of watermarked video frames

Figure 6 shows the graphical representation PSNR analysis outcome. The high PSNR values of the watermarked video frames calculated using the proposed technique represents better visual imperceptibility.

Table 3. Comparison analysis on basis of MSSIM parameter

Video name from which frame has been tested	Existing method	Proposed method
Aeroplane take-off	0.9834	0.9896
Athletics	0.9949	0.9978
Wildlife	0.9851	0.9905
Space shuttle	0.9891	0.9931
Australian grand	0.9972	0.9989
Cycling	0.9911	0.9952

Table 3 has shown the proposed method outperforms over the existing method in terms of parameter MSSIM.

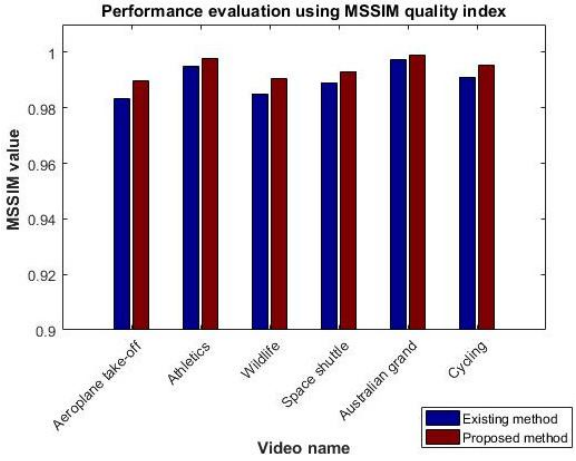

Fig. 7: Graph representing MSSIM value of watermarked video frames

Figure 7 shows the graphical representation MSSIM analysis outcome. The high MSSIM values of the watermarked video frames calculated using the proposed technique represents better invisibility of the hidden data is achieved.

Table 4. Comparison analysis on basis of NCC parameter

Video name from which frame has been tested	Existing method	Proposed method
Aeroplane take-off	0.9998	1.0000
Athletics	0.9998	1.0000
Wildlife	0.9998	1.0000
Space shuttle	0.9998	1.0000
Australian grand	0.9999	1.0000
Cycling	0.9998	1.0000

Table 4 has shown the proposed method outperforms over the existing method in terms of parameter NCC.

Experiments have conducted on different frames of video 'Aeroplane take-off.wmv' for authentication evaluation of the proposed scheme.

Table 5. Authentication analysis in terms of NCC parameter

Frame number	Parameters while extracting watermark using a true key			Parameters while extracting watermark using a fake key		
	PSNR	MSSIM	NCC	PSNR	MSSIM	NCC
15th	42.6419	0.9896	**1.0000**	42.6419	0.9896	**0.7203**
60th	42.8278	0.9966	**1.0000**	42.8278	0.9966	**0.5637**
105th	42.6556	0.9897	**1.0000**	42.6556	0.9897	**0.7811**
150th	44.0137	0.9990	**1.0000**	44.0137	0.9990	**0.6690**
195th	44.1808	0.9990	**1.0000**	44.1808	0.9990	**0.4955**
240th	43.0922	0.9948	**1.0000**	43.0922	0.9948	**0.6328**

Table 5 has shown no effect in PSNR and MSSIM values but a large distortion in NCC values that means while extracting watermark by an unauthorised user without knowing actual key, the extracted watermark looks like noise. The NCC values are highly degraded. This means that the proposed scheme is secured, since sensitive to key so only authorized user can extract the true watermarked information. This shows that no rogue user can identify the digital fingerprints if mounts attack on the proposed scheme which makes the proposed scheme robust against the collusion attack.

7. CONCLUSION

In this paper, a DCT based blind video watermarking scheme robust against collusion attack is proposed. This research work designs the digital fingerprints in the DCT domain which are embedded into the video frame and uniquely recognizes the authenticated user. The proposed scheme is visually imperceptible as quality of the video frames is not perceptually affected even if watermark is embedded. Moreover, the scheme is secured as a secret key is used while embedding watermark in random blocks and the same key is needed at the time watermark extraction. The experimental results and comparative analysis has shown the better performance of the proposed scheme over the existing scheme in terms of quality index metrics. It is concluded that no rogue user can identify these digital fingerprints if mounts attack on the watermarked video which makes the proposed scheme robust against the collusion attack. As a result, not any illegal copy of the original content can be produced by the culprits. Thus, piracy control in digital fingerprinting mechanism is achieved.

In future, work can be done while concentrating on further performance improvement of the proposed scheme. Furthermore, the current proposed scheme can be made robust against a number of attacks on a single platform. Moreover, the proposed scheme can be extended to more secure system by compressing the watermark before embedding. This will take more effort to break the system which leads to high security.

8. REFERENCES

[1] Boneh, D., and Shaw, J. 1996. Collusion-Secure Finger printing for Digital Data. IEEE Transactions on Information Theory. 44(5): pp.1897-1905.

[2] Barni, M., Bartolini, F., Cappellini, V., and Piva, A. 1998. A DCT- Domain System for Robust Image Watermarking. Signal Processing. vol.66: pp.357-372.

[3] Khayam, S. A. 2003. The Discrete Cosine Transform: Theory and Application. International Journal of Computer Applications. 49(10): pp.766-783.

[4] Kaur, G., and Kocchar, A. 2013. Transform Domain Analysis of Image Steganography. International Journal for Science and Emerging Technologies. 6(1): pp.29-37.

[5] Dzwonkowski, M., Rykaczewski, R., and Czaplewski, B. 2014. Digital Fingerprinting Based on Quaternion Encryption for Image Transmission. Article in Pattern Recognition Letters. vol.46: pp.11–19.

[6] Manaf, A. A., Boroujerdizade, A., and Mousavi, S. M. 2016. Collusion Resistant Digital Video Watermarking for Copyright Protection Application. International Journal of Applied Engineering Research. 11(5): pp.3484-3495.

[7] Karmakar, A., Phadikar, A., Phadikar, B. S., and Maity, G. K. 2016. A Blind Video Watermarking Scheme Resistant to Rotation and Collusion Attacks. Journal of King Saud University-Computer and Information Sciences. 28(2): pp.199-210.