computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

FRAME SELECTIVE AND DYNAMIC PATTERN BASED MODEL FOR EFFECTIVE AND SECURE VIDEO WATERMARKING

Kapil Juneja [1], Shaloo Bansal [2]

[1] Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, Haryana,124001, India
Email: kapil.juneja81@gmail.com, kapil.juneja.1981@ieee.org
[2] Department of Electronics and Communication, Faculty of Engineering & Technology, Mewar University, Rajasthan, India
Email: shaloobansal@gmail.com

Paper history:
Received 11 December 2018
Received in revised form 3 March 2019
Accepted 14 June 2019
Available online 30 June 2019

Keywords:
video watermarking;
histogram shift;
ECC;
dynamic pattern;
secure.

Abstract: Video watermarking enables the users to share the digital contents in public domain without any issue. However, video watermarking is also infected by various attacks that can even destroy the hidden watermark. The security, robustness and reliability are the key challenges of any Video watermarking technique. In this paper, such a robust and dynamic video watermarking framework is presented that can handle most of the existing issues. In this framework, the video is hiding on the selective frames and the preference of frames is done based on structural feature evaluation. After performing the frame selection, the featured analysis is accomplished on each frame to identify the effective cover blocks. The structure feature analysis based rules are applied to identify the most secure region over the frame. In the final stage, the histogram shift method is applied to perform data hiding. To improve the security, instead of hiding the complete image, the ECC (Elliptic Curve Cryptography) encrypted image is watermarked within the video frames. The analysis is performed on real time videos. The analysis results are generated in terms of MSE (Mean Square Error), PSNR(Peak Signal to Noise Ratio), SSIM (Structural Similarity Measure) and BCR (Bit Correct Ratio) parameters. The results identified that the proposed model has improved the effectiveness, robustness and security against various attacks. The comparative results are also validated against the DCT and DCT-SVD based video watermarking methods.

1. INTRODUCTION

Videos are gaining the popularity in terms of telefilms, advertisements, lectures, product or company endorsements, etc. These all kinds of videos are the proprietary of an individual or firm. Even though, these firms and persons want to circulate these videos in public domain to increase the popularity, publicity and profit. Anyone can claim digital contents or alter it to benefit them. Watermarking is one such control to restrict the authentication and authorization of such publicly distributed contents. The video watermarking is getting popular in recent years to secure these digital contents from illegal claim and redistribution. In video watermarking, a distinct and proprietor signature is hiding within the video or video frames to prove the claim on video. Video watermarking is done in recent years by the researchers using different methods. These methods are specific to the application domain as well as algorithmic methods. The temporal features, spatio-temporal features, ROI (Region of Interest) explicit watermarking and frame selective watermarking are the common methods defined by the researchers to improve the watermark security [1].

Even after embedding the watermark within the videos can be affected by various attacks for either retrieving the watermark or destroying it [2]. The watermarking method should be robust and imperceptible to these attacks. The watermark can be visible or invisible. The standard video watermarking model and its extraction are shown in Fig. 1. The figure shows that the secret key specific video encoding is applied on original video at the source end to generate the watermarked video. This digitally secured video can be distributed in public domain. The authentication of these videos is verified by performing the watermark decoding from these videos. The figure has shown the block diagram of signing and retrieval of these videos through the watermarking method.

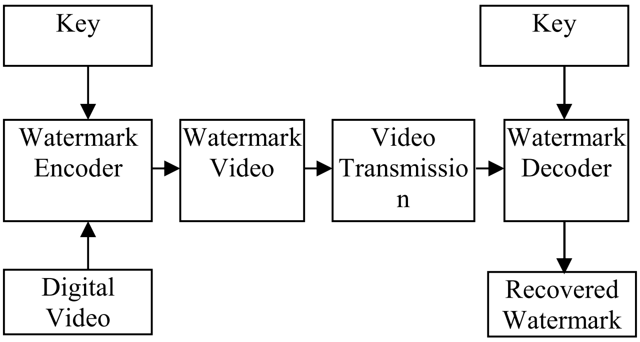


Figure 1 – Block Diagram of Video Watermarking

A good video watermarking algorithm must have some basic features and capabilities, including robustness, security, imperceptibility, etc. [3]. The robustness defines the capability of watermark video to bear different kind of attacks. The imperceptibility is associated to invisible watermarking and describes the safety of embedded contents within the video. The paper has proven the robustness and reliability of proposed watermarking method against different attacks on the videos taken from the different domain.

1.1 DWT (DISCRETE WAVELET TRANSFORMATION)

DWT is the decomposition method applied over the video frames for frequency level evaluation. In this work, two-level DWT is applied to extract the effective structural features. The DWT has divided the image in four frequency bands called HL, HH, LL, and LH as shown in Fig. 2. By applying the DWT decomposition, the low frequency features are identified from the frames. These features are able to identify the variation exist between the video frames and the threshold limit is applied to identify the effective cover frame.

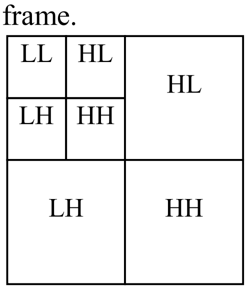


Figure 2 – 2 Level DWT

Fig. 2 shows the two-level decomposition applied in this research using DWT. The complete watermark image is divided in the smaller square blocks of size 16x16. In this research, the structural information of video frames is extracted and compared to identify the distinct frames from video. In first-level decomposition of DWT, the HH component is extracted as the content specification. This HH block is further decomposed using second level DWT. The HH component is selected after applying two-level decomposition on the extracted block to obtain the content and structural information from video frame. In this research, the Haar filter based DWT is applied for sub band extraction. Once the content information is extracted for two successive frames, the similarity analysis is done to identify the distinct cover frames.

1.2 ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

In this proposed watermarking model, the encoded watermark is embedded within the selective region of video frames. The elliptic curve is the alternative to the public key cryptography. This cryptography method is defined on the elliptic group with specification of group points. This cryptosystem is defined with specification of scalar multiplication and member point specification. The point multiplication is applied on watermark to generate the encoded image. The multiplication on the curve is done in this work using EW=k*W. Where EW is an encoded watermark and W is the actual watermark. k is the private key to perform the encoding. The encoding process is performed in Galois field that defines some other mathematical operation to generate the encoded image. This Galois field is the combination of addition and multiplication operations, which are applied in a sequence to generate the encoded image.

1.3 CONTRIBUTION OF THIS RESEARCH

In this research work, a framework is presented for optimizing the security, integrity and effectiveness of video watermarking. The main contributions of this proposed research method are listed below:

- In this work, the watermarked is performed in selected video-frames; it reduced the chances for detecting the cover video frames and improved the reliability.
- The content feature analysis is performed over the video frame for identifying the effective and dynamic region for storing the watermark.
- In effective region, the block-adaptive

histogram shift method is applied for hiding the pixel bits within cover region effectively.

- ECC is applied on watermark image for attaining the two-level security.

In this paper a frame and region selective method is proposed to improve the reliability and robustness of video watermarking. In this method, at first level, the DWT (Discrete Wavelet Transformation) based frame difference analysis is done to identify the cover frames. At second level, the structural feature analysis is done on frame blocks to identify the specific region over the frames. The enhancement of watermark security is done by applying the ECC (Elliptic curve cryptography) on watermark image. Finally, the histogram shift based method is applied to embed the encoded watermark within the selective region of selective frames. In this section, the basic aspects of video watermarking are discussed along with issues and characterization. In section II, the contribution of researchers is presented to handle various issues of watermarking using different algorithmic methods and for distinct application domains. In section III, the proposed watermarking model is presented with functional description. The algorithm and the operational characterization are also provided in this section. In section IV, the analytical results are provided on a sample video set which is taken from different domains. The comparative results are also provided for attacked and non-attacked watermark to verify the reliability of the proposed model. In section V, the conclusion of this research is presented.

2. RELATED WORK

In the recent years, the usage of social media and distribution of various image and video contents in public domain has increased the requirement to sign these digital contents. Researchers have defined different methods to improve the security, robustness and reliability of video watermarking. In this section, the work provided by earlier researchers to improve the video watermarking is provided and discussed. The scope, behavior and features of watermarking method and their types were discussed [4]. A comprehensive review for various video watermarking methods was provided [5]. The main contribution of researchers is identified in terms of frame selection, region selection and data hiding methods. In this section, the improvements and methods investigated in the earlier study in recent years for each category are discussed.

The researchers have extracted the different kind of features and feature regions to improve the reliability of video watermarking. Kerbiche et al. [2] have extracted the feature region from videos using crowd sourcing technique. In this approach, the mobility of an object was identified and considered as the feature region to hide the watermark within video frames. The mosaic pattern was generated as the cover region to improve the reliability of watermarking method. Gupta et al. [6] have used the Group Search Optimization (GSO) algorithm for selection of the frames and the cover region to hide the watermark within video. The optimized search method has performed the resource level analysis to identify the best-fit region over the video frames. Rasti et al. [7] identified the movement over the video to acknowledge the cover frames. The frame and region based evaluation is done using block entropy and average entropy features. The evaluation results identified the effectiveness of work against various attacks.

In video watermarking, the frame selection is another key approach, which is improved by the researchers to enhance the capacity, reliability and robustness of watermarking methods. Bhardwaj et al. [8] have used a significant selection and quantization method to improve the robustness of video watermarking. Author used the Lifting Wavelet Transformation (LWT) to identify the noteworthy frames. Later, the quantization method was applied to hide the watermark within the selected frames. A cuckoo Search [9] method was investigated to improve the scene change detection within videos. The DCT (Discrete Cosine Transformation) is combined with cuckoo search to detect the cover frames. Finally, DWT was applied to add the watermark in selected frames. Himeur et al. [10] used the GMSD (Gradient Magnitude Similarity Deviation) to identify the key frames. Once the frames are identified, the chaotic encrypted watermark is hiding using DWT and SVD (Singular Value Decomposition) based double transformation method. The encouraging results were obtained in terms of robustness, imperceptibility and capacity of watermarking. Shukla et al. [11] have applied the statistical measures to identify the scene change over the video. Once the scene is identified, the Haar wavelet was used with LH and LL sub bands to hide the watermark within video. Author achieved the better robustness and channel capacity using the proposed approach. Vural et al. [12] have identified the motion compensated frames based on the smoothness exist within continuous video frames. The block adaptive evaluation was also conducted to identify the pixel distortion and use it as the cover pixel for effective data hiding within videos.

Some of the researchers have provided various decomposition, bit specific and quantization method methods to improve the reliability and robustness of video watermarking. Bhardwaj et al. [13] have used the DWT, and DCT based sub-sub bands to perform video watermarking. The frame rate evaluation adaptive decomposition method was applied to enhance the strengths of video watermarking. Velickovic et al. [3] had applied the DWT-SVD (Discrete Wavelet Transform-Singular Value Decomposition) based watermarking within the chrominance channel of videos. Author also applied the GMSAT (Generalized Multi-Stage Arnold Transformation) based scrambling on watermark image to improve the security aspect. Gangarde et al. [14] used the PLBT (Pixel Location based Technique) to improve the robustness and imperceptibility of video watermarking. The spatial evaluation was also performed for selection of the cover video frames. The method reduced the complexity and improved the PSNR value effectively. Cai et al. [15] used the quantized discrete sine transform (QDST) coefficient block evaluation to reduce the error propagation and to improve the watermarking reliability. The luminance prediction unit was also defined on the textural features to identify the embedding region and to improve the security. Adul et al. [16] have provided the comparative evaluation of DWT and SVD methods of video watermarking. Author also presented a hybrid method to improve the robustness of video watermarking against various attacks. Ghalejughi et al. [17] have combined hyperbolic function with DT-CWT (Dual Tree Complex Wavelet Transform) to improve the multiplicative watermarking method. Author also used the chrominance channel to improve the quality of watermarking method. Kadu et al. [18,19] has transformed the spatial domain to frequency domain using DWT to achieve the effective copyright protection. Author used the low-frequency part (LL) sub-band as the cover to hide a watermark image within videos. Alenizi et al. [20] combined the DWT with HEVC (High-Efficiency Efficiency video Encoding) to improve the perceptual invisibility and robustness of video watermarking. Latha et al. [21] applied multi level DWT and SVM to improve the robustness and capacity of video watermarking.

Meenakshi et al. [22] applied the DCT-SVD based hybrid method for improving the robustness of video watermarking. Author recorded the watermark within video frames in zigzag fashion to improve the reliability and robustness. Sujatha et al. [23] used the bit-plane integrated scrambling using DWT approach for improving the security of watermark. The method achieved the effective results against various attacks. Mareen et al. [24] introduced the artificial distortions within videos and used these distortion regions for embedding the watermark. Author also used the encoder and compression method for enhancing the reliability and effectiveness of video watermarking. Upadhyay et al. [25] combined the DWT with LSB method for enhancing the capacity, robustness and imperceptibility of watermarking method. Author verified the method against noise, rotation, and cropping attacks. Li et al. [26] investigated a novel framework for embedding the watermark within the video by adding the artificial noise. Author applied the statistical modeling for locating the convincing region that can improve the security and reliability of watermarked contents. Afeefa et al. [27] utilized the shape of the histogram for hiding the secret watermark within image or video. The region-wise pixel-change analysis was performed by the author for inserting the watermark secretly within video. Bahrami et al. [28] used the visual-cryptography with SURF (Speed-Up Robust Features) for improving the performance and stability of video watermarking. Esfahani et al. [29] used the Dual-Tree complex wavelet transform (DTCWT) method for hiding the watermark within the low-frequency coefficients of the chrominance channel of video-frames. The spatial domain based method was defined for improving the reliability of the watermarking method.

In this paper, the partial-watermark is hiding within the selected frames. DWT based feature evaluation is conducted for frame-selection. The block-adaptive histogram shift method is applied for hiding the watermark within video frames. In next section, the algorithmic process and functional description of proposed model are provided.

3. RESEARCH METHODOLOGY

The authority, security and access rights of some digital contents can be secured by inserting the watermark within the image or video. The video watermarking can sign the rights of the video for an individual or firm. The watermarking method can affect the quality of the cover as well as can affect the watermark while retrieving it.

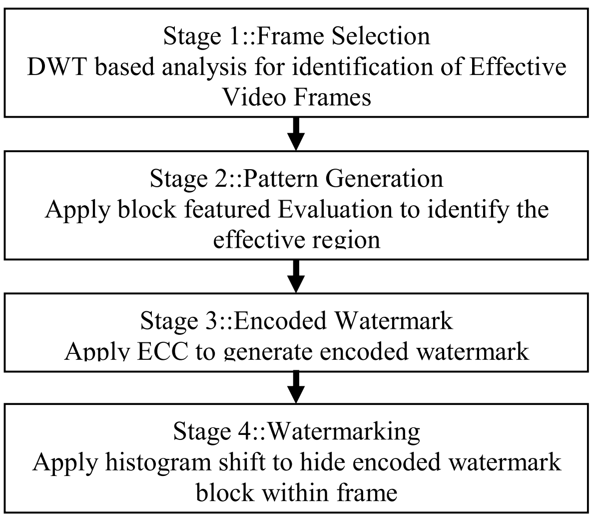


Figure 3 – Work Stages of Proposed Video Watermarking Model

Various kinds of attacks, communication behavior and deficiencies can affect the quality of distributed watermarked video. In this paper, a secure, dynamic and reliable video watermarking method is suggested. The proposed watermarking method accepts the cover video and watermark image as input. The method identified the effective frames and region from the cover video and hides the encoded watermark within selective video frames. The associated work stage of this proposed watermarking model is shown in Fig. 3. The Fig. 3 shows that the proposed model is divided into four main work stages, which are applied on cover video, watermark image or on both. At the earlier stage, the video file is processed, and the analysis is done on the continuous frames to identify the effective cover frames. In this stage, the DWT based analysis is done to identify the frames with scene variation.

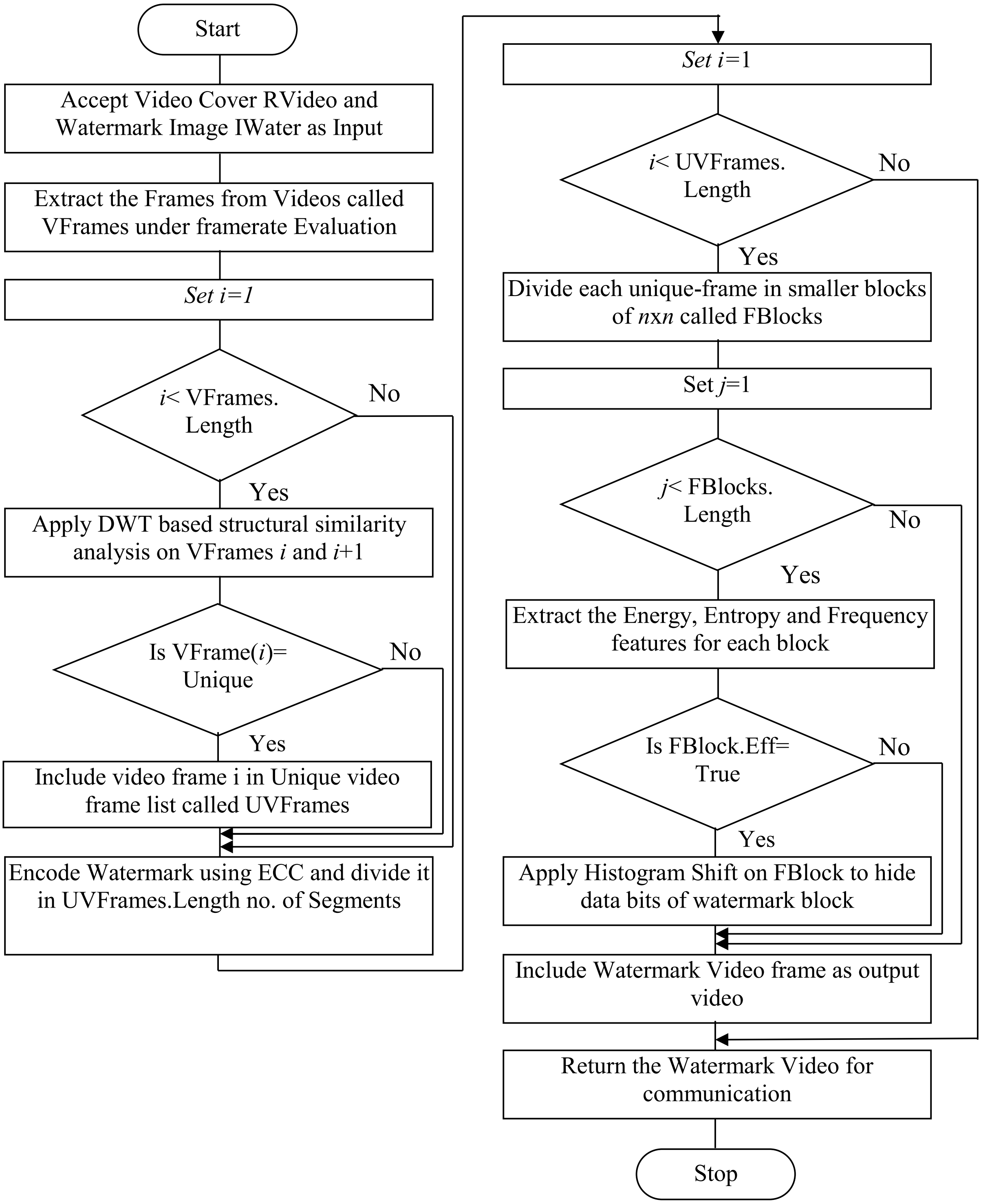


Figure 4 – Functional Flow of proposed Video Watermarking model

The decomposition measure analyzes the intensity difference between the frames and as the difference is larger than an acceptable limit, the frame is considered as the cover frame. Once the effective frames are shortlisted, the individual frame analysis is done. The shortlisted video frames are divided into smaller rectangular blocks. The analysis of each block is done using entropy, energy and frequency parameters. The dynamic evaluation is performed on this parameter to consider as the effective cover blocks. The pattern based weighted analysis rule is defined to perform the election of these blocks. These parameters are able to identify the rich areas over the video frame that can hide the information more secretly and safely. These regions will not be affected by different kind of attacks. The parameters considered for the identification of such valuable regions are computed using the equations given below.

$$\text{Energy} = \sum_{i=1}^{h}\sum_{j=1}^{w}[IBlk(i,j)^2], \quad (1)$$

$$\text{Entropy}= \sum_{i=1}^{h}\sum_{j=1}^{w} IBlk(i,j)log_2[IBlk(i,j)], \quad (2)$$

$$\text{Frequency}=\sum_{i=1}^{h}\sum_{j=1}^{w} i*j*[IBlk(i,j)], \quad (3)$$

where, *IBlk* is Image Block, *IBlk*(*i,j*) is the intensity of pixel (*i,j*), h,w are height and width of image blocks.

After evaluating these features, the rule is developed to identify the eligibility of the block as the cover.

Fig. 4 has provided the functional description of the proposed video watermarking model. The figure shows that the video file and the watermark-image are taken as input. The sequential process on video file is performed for frame-separation, effective region extraction and the watermark hiding within the selected region. Table 1 has provided the algorithm to process the cover video and watermark image and to authenticate the video in an effective way. The algorithm also defined the rule to process these features and to generate the dynamic cover region over the video frames. In this proposed model, one the effective region is extracted, the watermarking is performed using histogram shift method. In this method, the histogram for each block of the effective region is obtained. In this histogram, two subsequent peaks called h1 and h2 are identified. These peaks identify the high frequency regions for hiding the pixels within the block. The rules are defined for hiding the pixel watermark information within the video frame. If abs(h1-h2)>0, then the block is eligible for storing the watermark content. The immediate frequency points are computed to h1 and h2 called b1 and b2 for performing the histogram shift operation to hide watermark information. These peaks and the immediate peaks are processed for hiding the watermark content within the video frame. The rule for using these frequency bits for hiding the watermark image within video frame is shown in Table 1.

Another input taken in this framework is the watermark image. Instead of watermarking the image in its original form, the ECC (Elliptic curve cryptography) is applied over it to encode the image and to improve the reliability and security. Once the image is encoded, the image is divided into smaller segments based on the number of available cover regions. In the final stage, histogram based watermarking is applied. Each of the cover blocks is analyzed, and the frequency peaks are obtained from it. The histogram shift rule is applied on two peaks of image to hide the information bits within the blocks. This process is repeated on image blocks until the data bits are available for that particular frame.

Table 1. Feature Adaptive Video Watermarking Algorithm

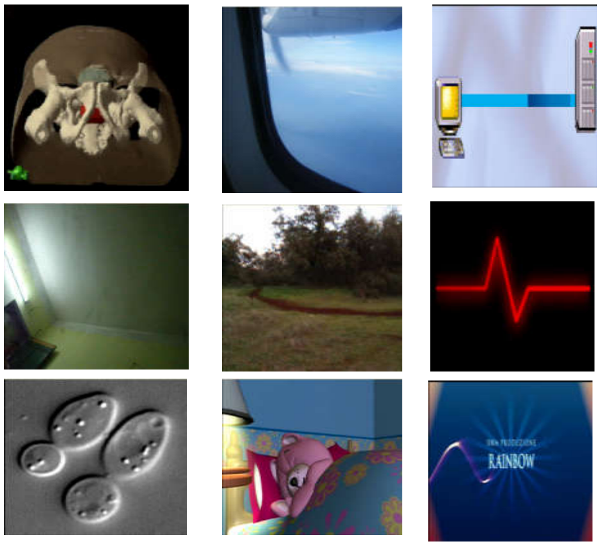
```
VideoWatermarking(RVideo,Watermark)
/*RVideo is the real time video that an organization
or individual want to protect from illegal access,
Watermark is the watermark image to sign the
digital video*/
Begin
1.   Status=Analyze(RVideo)
     /*Analyze the video format and quality*/
2.   If (Status=Yes) /*Video is eligible to use as
     cover video*/
     Begin
3.   VFrames=Div(RVideo, FrameRate)
     /*Extract the video frames from RVideo
     based on Framerate*/
4.   VFrames(1).Select=True /*First Frame is
     selected*/
     St=1
5.   For i=2 to VFrames.Length
     /*Process all the frames*/
     Begin
6.   VFrames(i).Select
     =DWTCompAnalysis(VFrames(i),VFrames(
     St))
     /*Identify the similarity ratio for two
     continuous frames using DWT*/
     End For
     End If
7.   EWatermark=ECC (Watermark) /*Apply
     ECC to encode the image*/
8.   SWatermark=
     EWatermark/VFrames.Length /*Generate
     the watermark segments based on available
     cover frames*/
9.   ForEach frame in VFrames
10.  FBlocks=GenerateBlocks(VFrame,Size)
     /*Generate rectangular blocks for each
```

```
        frame*/
11.     For i=1 to FBlocks.Length
12.     En=Entropy(FBlocks(i))
        Freq=Frequency(FBlocks(i))
        Energy=Energy(FBlocks(i))
        /*Extract the features for analysis of block*/
13.     If (En>Th1 And Freq>Th1 And
        Energy>Th1) /*Defines rules for block
        Selection*/
                FBlocks(i).Select=True
        ElseIf (En>Th2 And Freq>Th2)
                FBlocks(i).Select=True
        ElseIf (Energy>Th2 And Freq>Th2)
                FBlocks(i).Select=True
        Else (Energy>Th3 || Freq>Th3)
                FBlocks(i).Select=True
        End If
14.     Hist=Histogram(FBlocks(j)) /*Generate the
        histogram on selected block*/
15.     [p1 p2]=GetPeaks(Hist) /*Get Peaks from
        Histogram*/
16.     DBits=ExtractNxtBits(SWatermark) /*Get
        next bits from blocks of secure watermark*/
17.     FBlock(j)=HistogramShift (FBlock(j),
        DBits,p1, p2) /*Apply histogram shift for
        data hiding*/
        End For
        End For
End
```

After hiding the watermark within the video, the digital video can be shared in the public domain. If someone uses the contents illegally or without the permission, the watermark can be extracted to validate the authorization on that video. The watermark recovery process is applied with same algorithmic model to extract the hidden watermark from the image. The identification of effective frames, generation of block pattern and reverse histogram shift rules are applied to retrieve the watermark bits from the image. The decryption process is applied on extracted watermark to obtain the watermark in its original form.

4. RESULTS AND DISCUSSIONS

The paper has provided the watermarked authentication for real time videos. The work is capable of hiding the watermark within selective frames of videos. The presented dynamic pattern based video authentication model is implemented in Matlab environment. The model is applied on real time videos with different frame count. A sampleset of videos considered in this research is shown in Fig. 5. Figure is showing the nine cover videos and one watermark image. The analytical evaluation is conducted on the larger video sets of 10, 20 and 30 videos. All the videos considered in this research are in AVI (Audio Video Interleaved) format with the frame rate 10 fps.



(a) – Cover Videos

(b) : Watermark Image

Figure 5 – Sample Videos for Video Watermarking

The cover videos which are considered in this research are high-resolution color videos. The resolution of this particular sampleset and video lengths is provided in Table2.

Table 2. Features of Sample Cover Videos

Cover Videos	Video Size (In Seconds)	Resolution	Number of Video Frames
Video1.avi	4	240x180	37
Video2.avi	2	640x480	19
Video3.avi	<1	174x170	12
Video4.avi	1	320x240	14
Video5.avi	2	320x240	21
Video6.avi	5	480x320	56
Video7.avi	19	428x448	218
Video8.avi	8	320x240	69
Video9.avi	7	720x576	57

Table 2 has provided the features of nine sample videos. The matlab functions are applied to extract the frames from videos. The video size in seconds and the number of video frames extracted are shown in the figure. These all frames are not considered as cover frames. The DWT based feature analysis is performed to identify the changes in continuous frames. Based on the adaptive limit, the cover frames are identified. The analytical results are generated on different samplesets with and without the existence of diverse attacks. The analysis parameters are provided in section 4.1.

4.1 ANALYSIS PARAMETERS

The analytical observation is applied on three different samplesets to verify the quality of recovered watermark. The effectiveness and reliability of proposed watermarking method are validated using MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), BCR (Bit Correct Ratio) and Structural Similarity Ratio (SSIM).

4.1.1 PSNR

PSNR is the mathematical measure used to analyze the quality of an image. This measure applies the pixel difference evaluation between the input and reconstructed image. In this work, the recovered watermark image is the reconstructed image which is compared with input watermark for the measurement. The PSNR formulation is shown in equation (4)

$$\text{PSNR} = 10 \log \frac{S^2}{MSE}, \tag{4}$$

where, s=255 for 8 bit image/image.

4.1.2 SIMILARITY RATIO

The similarity index is another parameter that provides the block specific evaluation on original and recovered watermark. The mean and standard deviations are the parameters applied with luminance, contrast evaluation. The similarity analysis between source(X) and reconstructed (Y) image is provided in equation (5)

$$\text{Sim}=\frac{(2\mu_X\mu_Y+c1)(2\sigma_{XY}+c2)}{(\mu_X^2+\mu_Y^2+c1)(\sigma_X^2+\sigma_Y^2+c2)}. \tag{5}$$

4.1.3 MSE

MSE is evaluated on source and reconstructed image by averaging the squared intensity of image pixels. The error rate evaluation is obtained by using this measure. The MSE equation is provided in equation (6)

$$\text{MSE} = \frac{1}{NM}\sum_{i=1}^{M}\sum_{j=1}^{N} e(i,j)^2, \tag{6}$$

where, *e*(*i*,*j*) is the error difference between original and recovered watermark image. *N*, *M* is the size of images.

4.1.4 BCR

The measure can identify the ratio of correctly extracted bits from the cover image. The BCR evaluation is provided through equation (7) and the mapping between source (X) and recovered image (Y) is

$$\text{BCR} = \frac{1}{L}\sum_{i=1}^{L}\frac{1}{X(i)\otimes Y(i)} \text{ x } 100, \tag{7}$$

where, L is size of image/object.

4.2 COMPARATIVE ANALYSIS (WITH AND WITHOUT ATTACK)

In this section, the analysis results are generated on the sample files shown in Fig. 5 and described in Table 2. The analysis results are generated for the parameters described in section 4.1. The watermarked videos are shared in public domain and accessed by different people and media groups. The intruder in public domain can try to retrieve or destroy these watermarks to take the claim these videos. These commercially distributed videos can suffer from various kinds of attacks that can disrupt the hidden watermark information. In this research, the robustness of the proposed watermarking model is verified against some of these attacks. In this section, the analysis results are generated for attacked and non-attacked videos. The attacks considered in this research work for evaluation are Unsharp attack, Salt & Pepper Attack, Blur Attack and Gaussian Attack. The unsharp attack sharp the edges of the image and highlight the structural information. It increases the contrast over the image and highlights the effective region. The adjustment on light and dark regions is done to highlight the structural information. If the structural information is used to hide the information, it can be disturbed by this attack. Gaussian noise is another attack considered in this work. The Gaussian noise is the statistical noise which is spread over the image using normal distribution. While the video is communicated over the network channel, it can be affected by natural sources. This noise distorts the contents and information over the image by adding the noise contents. Another noise considered in this research is Salt & Pepper noise. This noise applies two impulse functions at discrete location to distribute the noise elements over the image. These impulse functions distributed the noise of different intensity and color. The pixel level probabilistic disruptions occur in this image and destroy the image contents. Blur is the statistical filter which is applied over the image nonlinearly. This attack smoothens the region block by taking some aggregative observation. In this work, the median filter is applied to function as the blur attack. This filter is rank based function applied on the region block and replaces the region pixels by the average value of that region.

The robustness and reliability of proposed watermarking method are verified on these above-described attacks. The observations are taken on sample videos in existence of each attack as well as in no-attack situation. The comparative results are generated against Shaloo et al. [1]. Table 3 has provided the analysis results for nine sample videos against MSE. The table has provided the numerical observations for attack and no-attack watermark videos. The comparative results show that the proposed approach has significantly reduced the MSE value almost for each experimentation as compared to the Shaloo et al. [1]. The table shows that the MSE value is increased in existence of different attacks, but it is lesser than the observations obtained for Shaloo et al. [1]. It shows that the proposed watermarking model has significantly reduced the error rate and improves the reliability.

Table 3. MSE based Comparative Analysis (With & Without Attacks)

	No Attack		Unsharp Attack		Salt and Pepper		Blur Attack		Gaussian	
Video File	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. ([1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed
Video1.avi	0.012	0.013	0.0761	0.06902	0.29279	0.14326	0.11235	0.08632	0.11343	0.09563
Video2.avi	0.029	0.026	0.05442	0.04724	0.30543	0.16326	0.22662	0.14632	0.34456	0.3263
Video3.avi	0.028	0.023	0.10532	0.08963	0.29305	0.18632	0.33127	0.21639	0.12269	0.10563
Video4.avi	0.0213	0.019	0.33856	0.16356	0.09119	0.0645	0.1245	0.08763	0.18092	0.1263
Video5.avi	0.0196	0.018	0.02908	0.01063	0.14556	0.07963	0.18007	0.09756	0.02225	0.01264
Video6.avi	0.0204	0.018	0.14838	0.08796	0.08506	0.07263	0.01802	0.00463	0.22731	0.17963
Video7.avi	0.02432	0.022	0.29901	0.16384	0.14491	0.08963	0.34088	0.18965	0.28701	0.25635
Video8.avi	0.0218	0.021	0.10473	0.06489	0.09571	0.04569	0.19365	0.06896	0.27278	0.21456
Video9.avi	0.02634	0.022	0.30442	0.18963	0.237	0.17896	0.24006	0.11362	0.14636	0.07896

PSNR is another parameter taken in this research to validate the significance of proposed watermarking model. PSNR can analyze the quality of the image against the noise or the disruptions occur at the content level. Higher the PSNR value, more significant the watermarking method is considered. Table 4 has provided the analysis results using PSNR values obtained for nine videos. The results show that the PSNR value is higher than shaloo et al. [1] for all attacked and non-attacked videos. It shows that the proposed watermarking model is more robust against the different kind of noise or content specific attacks.

Table 4. PSNR based Comparative Analysis (With & Without Attacks)

	No Attack		Unsharp Attack		Salt and Pepper		Blur Attack		Gaussian	
Video File	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed
Video1.avi	67.339	66.9914	59.317	59.7411	53.465	56.5696	57.625	58.7697	57.584	58.3249
Video2.avi	63.507	63.9811	60.773	61.3877	53.282	56.0019	54.578	56.4778	52.758	52.9946
Video3.avi	63.659	64.5135	57.906	58.6063	53.461	55.4282	52.929	54.7784	57.243	57.8929
Video4.avi	64.847	65.3433	52.835	55.994	58.531	60.0352	57.179	58.7043	55.556	57.1168
Video5.avi	65.208	65.5781	63.495	67.8655	56.501	59.12	55.576	58.2381	64.658	67.1151
Video6.avi	65.035	65.5781	56.417	58.6878	58.834	59.5196	65.572	71.475	54.565	55.587
Video7.avi	64.271	64.7066	53.374	55.9866	56.52	58.6061	52.805	55.3513	53.552	54.0425
Video8.avi	64.746	64.9086	57.93	60.009	58.321	61.5326	55.261	59.7448	53.773	54.8153
Video9.avi	63.925	64.7066	53.296	55.3517	54.383	55.6032	54.328	57.5763	56.477	59.1567

BCR defines the number of bits correctly retrieved by applying the watermark recovery. It is the ratio between the number of bits retrieved accurately and the total number of bits in the image. The higher the BCR ratio obtained through watermarking method, more reliable the method is considered. The comparative results of proposed method for BCR evaluation are provided in table 5 for attacked and non-attacked watermarked videos. The table shows that the attack has increased the bit loss over the image, but it is still lesser than the values obtained against Shaloo et al. [1]. It shows that the significant gain in accuracy and reliability is achieved using proposed watermarking method. This method can measure the structural and descriptive information of the watermark image.

Table 5. BCR based Comparative Analysis (With & Without Attacks)

	No Attack		Unsharp Attack		Salt and Pepper		Blur Attack		Gaussian	
Video File	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed
Video1.avi	53.24	57.2031	45.67	54.676	55.38	58.0143	42.35	53.9017	52.54	54.9834
Video2.avi	68.62	69.3425	58.79	63.1218	53.03	61.5842	63.19	62.3057	76.00	65.7098
Video3.avi	72.62	71.276	46.24	65.1838	73.37	72.2495	70.67	51.6639	56.64	66.9201
Video4.avi	61.62	67.8945	79.58	66.8034	61.96	64.323	65.13	38.4375	44.86	65.1438
Video5.avi	58.64	63.4849	64.07	63.2478	45.32	59.6727	60.37	37.9654	44.03	53.2011
Video6.avi	68.96	70.73	74.63	72.2451	64.77	66.831	68.06	47.0801	56.53	65.181
Video7.avi	60.22	64.6753	48.55	57.098	75.72	69.6833	65.11	34.7269	63.58	63.1243
Video8.avi	58.63	61.0248	49.03	56.2865	58.11	69.6762	79.80	76.624	77.72	66.3982
Video9.avi	63.31	67.8417	68.64	67.0645	57.87	60.8689	71.67	70.632	49.21	72.4703

The structural information is the most sensitive and content specific information, which can recognize the watermark object even if distortion exists. SSIM is the measure applied to measure the systemic information for the retrieved watermark. Table 6 has provided the comparative results for proposed and Shaloo et al. [1] methods. The higher the SSIM value, It shows that the more chances to match the retrieved watermarked. The results show that the SSIM value obtained for the proposed approach is significantly higher the values obtained using Shaloo et al. [1] method. The proposed approach has outperformed the existing method for both attacked and non-attacked videos.

Table 6. SSIM based Comparative Analysis (With & Without Attacks)

	No Attack		Unsharp Attack		Salt and Pepper		Blur Attack		Gaussian	
Video File	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed	Shaloo et al. [1]	Proposed
Video1.avi	0.627	0.7057	0.5388	0.64018	0.0114	0.54744	0.7537	0.4184	0.3137	0.62444
Video2.avi	0.8632	0.8556	0.9671	0.89377	0.2714	0.6472	0.6633	0.31528	0.9365	0.61025
Video3.avi	0.785	0.789	0.8519	0.80274	0.8104	0.0767	0.3608	0.68024	0.8344	0.46914
Video4.avi	0.821	0.8384	0.7733	0.83444	0.4429	0.70796	0.7262	0.84251	0.3473	0.0229
Video5.avi	0.863	0.8986	0.8371	0.86452	0.0947	0.48648	0.0513	0.07716	0.4518	0.55732
Video6.avi	0.891	0.8867	0.8426	0.85079	0.4809	0.88133	0.9744	0.1371	0.5201	0.02725
Video7.avi	0.728	0.8087	0.2428	0.68889	0.8126	0.64339	0.2588	0.81984	0.8539	0.52541
Video8.avi	0.731	0.7436	0.9693	0.6129	0.5992	0.68079	0.2841	0.05145	0.7405	0.60887
Video9.avi	0.697	0.825	0.0792	0.71653	0.1619	0.13471	0.1374	0.50684	0.908	0.647

The section has provided the analytical observations for the real time videos of different size and domains. The watermarked videos can be affected by distinctive kind of attacks. The analysis is conducted to observe the quality of retrieved watermark. The content, information bits, error rate and structural information are observed to verify the robustness and reliability of the proposed model. The experiments conducted in this section have observed that the proposed method has reduced the error rate significantly and improved the SSIM, BCR and PSNR ratio. These comparative results collectively verified that the proposed approach has improved the reliability and robustness effectively for proposed video watermarking method.

4.3 VALIDATION AGAINST STATE-OF-ART METHODS

The comparative evaluation of the proposed watermarking model is done against the DCT [30] and DCT-SVD [30] based methods. The analysis results are computed against the PSNR parameter. Figure 6 has provided the validation results against these state-of-art methods.

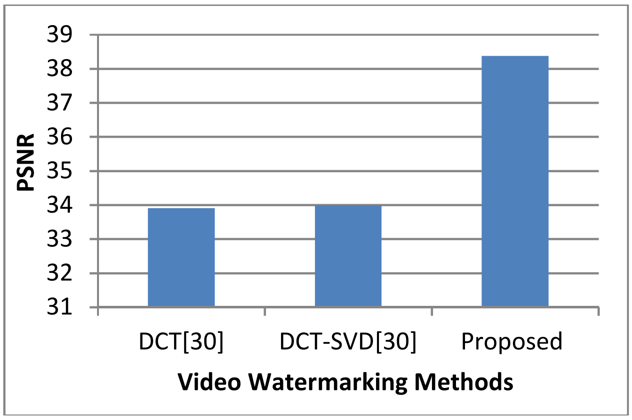


Figure 6 – Comparative Analysis

Figure 6 provides the comparative evaluation of the proposed watermarking model against the state-of-art methods. The results shows that DCT achieved the 33.91 and DCT-SVT achieved the 33.99 PSNR value, whereas the average PSNR value is 38.37. It shows that the proposed method has improved the performance over existing methods significantly.

5. CONCLUSION

In this paper, a frame selective and dynamic pattern based model is presented to improve the effectiveness of video watermarking. The model is defined to hide the image watermark within the selective video frames. Instead of hiding the actual watermark, an encrypted watermark is hide to improve the security and reliability against various attacks. The processing of this presented framework is covered in four stages. In first stage, the video frames analysis is done using DWT approach to identify the most effective cover frames. Once the frames are identified, the feature based analysis is performed on each video frame. In this stage, the effective region is identified over the video frame that can hide data effectively. In third stage, ECC cryptography is applied on watermark image to improve the security. The image is also divided in N segments based on the number of available frames. In the final stage, the histogram shift method is applied on blocks of video frames and watermark segments bits to perform data hiding. The proposed work is applied on nine real time videos taken randomly from web sources. The analysis is conducted in terms of MSE, PSNR, SSIM and BCR parameters. The comparative evaluation shows that the significant gain in PSNR, SSIM and BCR rate is obtained and the reduction in MSE is achieved. The results verify that the proposed model has improved the robustness and effectiveness of video watermarking.

6. REFERENCES

[1] S. Kikan and V.R. Singh, "Dynamic pattern based model for effective image-sequence watermarking,"*Journal of Emerging Technologies and Innovative Research*, vol. 5, no. 3, pp. 966-971, 2018.

[2] A. Kerbiche, S. Ben Jabra, E. Zagrouba, V. Charvillat, "A robust video watermarking based on feature regions and crowdsourcing," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26769-26791, 2018.

[3] Z.S. Velickovic, Z. Milivojevic, and M.Z. Velickovic, "A secured digital video watermarking in chrominance channel," *Proceedings of the 23rd International Scientific-Professional Conference on Information Technology (IT)*, Zabljak, 2018, pp. 1-4.

[4] M. Asikuzzaman and M.R. Pickering, "An overview of digital video watermarking," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2131-2153, 2018.

[5] B. Sridhar, "An investigation of different video watermarking techniques," *International Journal on Smart Sensing and Intelligent Systems*, vol. 10, no. 2, pp. 387-406, 2017.

[6] G. Gupta, V.K. Gupta, and M. Chandra, "An efficient video watermarking based security model," *Microsystem Technologies*, vol. 24, no. 6, pp. 2539–2548, 2018.

[7] P. Rasti, S. Samiei, M. Agoyi, S. Escalera, and G. Anbarjafari, "Robust non-blind color video watermarking using QR decomposition and entropy analysis," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 838-847, 2016.

[8] A. Bhardwaj, V.S. Verma, and R.K. Jha, "Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform," *Multimedia Tools and Applications*, vol. 77, no. 15, pp. 19659-19678, 2018.

[9] K. Aditya, A. Choudhary, A. Raj, and M. Sing, "Video watermarking based on Cuckoo search

and scene change detection," *Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, 2017, pp. 420-424.

[10] Y. Himeur and A. Boukabou, "A robust and secure key-frames based video watermarking system using chaotic encryption," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8603-8327, 2018.

[11] D. Shukla and M. Sharma, "A novel scene-based video watermarking scheme for copyright protection," *Journal of Intelligent Systems*, vol. 27, no. 1, pp. 47-66, 2018.

[12] C. Vural and B. Barakli, "Adaptive reversible video watermarking based on motion-compensated prediction error expansion with pixel selection," *Signal, Image and Video Processing*, vol. 10, no. 7, pp. 1225-1232, 2016.

[13] A. Bhardwaj and A. Khunteta, "Video watermarking equations using DWT and DCT sub-sub bands for secure transmission over communication channels: A research paper," *Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, 2017, pp. 436-440.

[14] M.A. Gangarde and J.S. Chitode, "Application of crypto-video watermarking technique to improve robustness and imperceptibiltiy of secret data," *Proceedings of the IEEE Fourth International Conference on Image Information Processing (ICIIP)*, Shimla, 2017, pp. 1-6.

[15] C. Cai, G. Feng, C. Wang, and X. Han, "A reversible watermarking algorithm for high efficiency video coding," *Proceedings of the IEEE 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Shanghai, 2017, pp. 1-6.

[16] V. Adul and E. Mwangi, "A robust video watermarking approach based on a hybrid SVD/DWT technique," *Proceedings of the IEEE International Conference AFRICON*, 2017, pp. 309-313.

[17] M. Ghalejughi and M.A. Akhaee, "Video watermarking in the DT-CWT domain using hyperbolic function," *Proceedings of the IEEE 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, Tehran, 2016, pp. 97-100.

[18] S. Kadu, C. Naveen, V.R. Satpute, and A.G. Keskar, "A blind video watermarking technique for indoor video content protection using discrete wavelet transform," *Proceedings of the IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, 2016, pp. 1-6.

[19] S. Kadu, C. Naveen, V.R. Satpute, and A.G. Keskar, "Discrete wavelet transform based video watermarking technique," *Proceedings of the IEEE International Conference on Microelectronics, Computing and Communications (MicroCom)*, Durgapur, 2016, pp. 1-6.

[20] F. Alenizi, F. Kurdahi, A. Eltawil, and A. Aljumah, "DWT-based watermarking technique for video authentication," *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, Cairo, 2015, pp. 41-44.

[21] S.B. Latha, D.V. Reddy, and A. Damodaram, "Digital video watermarking using DWT and singular values," *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS'16)*, New York, 2016, p. 5.

[22] K. Meenakshi, K. Swaraja, and P. Kora, "A robust DCT-SVD based video watermarking using zigzag scanning," *Soft Computing and Signal Processing*, pp. 477-485, 2019.

[23] C.N. Sujatha and P. Sathyanarayana, "DWT-based blind video watermarking using image scrambling technique," *Information and Communication Technology for Intelligent Systems*, pp. 621-628, 2018.

[24] H. Mareen, J.D. Praeter, G.V. Wallendael, and P. Lambert, "A novel video watermarking approach based on implicit distortions," *IEEE Transactions on Consumer Electronics*, vol. 64, no. 3, pp. 250-258, 2018.

[25] J. Upadhyay, B. Mishra, and P. Patel, "A modified approach of video watermarking using DWT-BP based LSB algorithm," *Proceedings of the IEEE International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, Indore, 2017, pp. 1-6.

[26] L. Li et al., "A novel framework of robust video watermarking based on statistical model," *Proceedings of the IEEE International Conference on Cloud Computing and Security*, 2018, pp. 160-172.

[27] P. Afeefa and I. Muhammed, "A histogram based watermarking for videos and images with high security," *Proceedings of the IEEE International Conference on Soft Computing Systems*, 2018, pp. 111-115.

[28] Z. Bahrami and F. A. Tab, "A new robust video

watermarking algorithm based on SURF features and block classification," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 327–345, 2018.

[29] R. Esfahani, M.A. Akhaee, and Z. Norouzi, "A fast video watermarking algorithm using dual tree complex wavelet transform," *Multimedia Tools and Applications*, pp. 1-17, 2018.

[30] S. Mawande and H. Dakhore, "Video watermarking using DWT-DCT-SVD algorithms," *Proceedings of the IEEE International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, 2017, pp. 1161-1164.

Kapil Juneja *is currently doing PhD in computer science and engineering at the M.D. University, Rohtak, Haryana, India. His research interests include image processing, biometrics, pattern recognition, computer networks, software engineering and machine learning.*

Shaloo Bansal *pursuing research work for gaining her PhD degree from Mewar University, Chittorgarh, Rajasthan, India. She has done her B.Tech and M.Tech in Electronics and Communication engineering. Her areas of interest are Digital Image processing and Electronics systems. She has teaching experience of 9 years. She has about ten research papers, to her credit, in National and International Journals and Conferences.*