


Fibonacci Based Key Frame Selection and Scrambling for Video Watermarking in DWT–SVD Domain

S. Ponni alias Sathya¹ · S. Ramakrishnan¹ 

Published online: 19 January 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract Video copyright is the technique for hiding sensitive data in digital video. This paper aims to introduce a new technique for video copyright namely Fibonacci based keyframe selection and scrambling for video watermarking in DWT–SVD. In this methodology, scene change detection technique is employed for identifying frequent changes in the scenes. In a specific frame, each scene is selected by using keyframes, which are generated by Fibonacci sequence. The initial seeds of the Fibonacci sequence are used as authentication key for generating keyframes. Based on the limitations of the scene changes the authentication keys are generated. The watermark is embedded only in specific frame of the changed scene in LH sub band. The secret image is scrambled using Fibonacci–Lucas transform. In embedding process, singular values (SVs) of the scrambled watermark block are added to the SVs of specific frames, produce the watermarked video collectively. In extraction phase, SVD is performed on the watermarked video to extract the scrambled watermark block from key frames. After that the extracted watermark blocks are collected together to yield the complete scrambled watermark. Later it is descrambled by using the secret keys to generate the original watermark. This method is blind since the host video is not required to extract the watermark. The experimental results show that the proposed methodology resists different image and video processing attacks. In addition, the proposed methodology improves the robustness and quality of both host video and watermark.

Keywords Video watermarking · Discrete wavelet transform (DWT) · Singular value decomposition (SVD) · Scene change detection · Fibonacci sequence · Image scrambling

✉ S. Ponni alias Sathya
sathyaashok2007@gmail.com

S. Ramakrishnan
ram_f77@yahoo.com

¹ Department of Information Technology, Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamilnadu, India

1 Introduction

In recent days, usage of multimedia and data utilisation has become inevitable in daily walks of life. The digital technology enables plethora of ways and means to access the digital data. But this transmission entails pirated forms. Digital data ownership has almost become a distant dream in these days. The watermarking is a unique technique used to protect digital data from illegal distribution. A watermark is a secret data inserted into objects like image, audio and video. Video watermarking is a technique which is used to offer authentication to the video content by embedding the watermark data to host video. As the image watermarking techniques are not applicable to the video data, the redundancy rate goes up.

Various kinds of video attacks are generally related to frame dropping, frame averaging, frame swapping, etc. Hence the watermark method ought be robust against all type of attacks [1, 2]. Digital watermarks and its techniques can be subdivided into various categories. Moreover, it can be classified based on application, source type (image watermarks, video watermarks, audio watermarks, text watermarks), human perception, and the technique used. Digital watermarks can be measured on the basis of certain properties such as fidelity, robustness, fragility, tamper resistance, data payload, complexity etc., [3, 4].

Various methodologies are developed in the recent past in order to provide authentication to video data. Each method has its own merits and demerits in terms of imperceptibility and robustness of the watermarking scheme.

Ejima and Miyazaki [5], embedded the watermark image into the LL sub band of the source video by using wavelet packets. The demerits of this methodology include, it is not robust against filtering, frame averaging and swapping and high complexity time.

Xu [6], proposed a 3D wavelet transform based blind watermarking algorithm. In this method, the host video is divided into three dimensional blocks. The watermark is embedded into the motive block of the source video. This method does not withstand against certain image and video processing attacks.

Al-Taweel and Sumari [7], proposed 3D-DWT domain based video watermarking using LL sub band for embedding process. Three level DWT was applied into LL sub band and there after the selected coefficients are embedded with the watermark. This algorithm does not withstand noise addition and frame processing attacks.

Reyes et al. [8], proposed Chaotic Mixtures based digital video watermarking in DWT Domain. In this algorithm, the binary pattern as a watermark was inserted into randomly selected scene blocks. DWT was applied in every scene. This method does not withstand certain attacks like frame processing and noise contamination.

Chetan and Raghavendra [9], proposed a DWT based video authentication. In this method, author has selected middle frequency band such as HL and LH sub band for embedding process. The DWT was employed for transforming the original video and the scrambled watermark was embedded into various scenes. This method does not resist against swapping and filtering.

Preda and Vizireanu [10], proposed a wavelet based video watermarking scheme, where the author employed two level decomposition by quantization method. The LH, HL and HH sub-bands were selected as binary image for watermark embedding. This method was not reported to be robust against certain frame based attacks.

Cruz-Ramos et al. [11], proposed a robust video watermarking scheme, wherein the author has used DWT for video frame transformation, watermark as company trademarks and owner's logotype that are visually recognizable patterns. This algorithm was not robust against geometric distortions and filtering attacks.

Preda and Vizireanu [12], did propose wavelet-based watermarking scheme for video copyright protection. In this algorithm, the binary image is chosen as a watermark. The embedding process was done in the middle level sub band. The author has employed a combination of quantization with spread spectrum based watermarking. This method was not resistant against certain frame based attacks.

Faragallah [13], has suggested singular value decomposition based video watermarking in the DWT domain. He has transformed the video frames with the DWT in dual resolution levels. The watermark was hidden in the SVD transformed video. An error correction code was found and the watermark was embedded with spatial and temporal redundancy. This method is resilient against image processing attacks but not against the video processing attacks like filtering, frame dropping and swapping.

Naved and Rajesh [14], have proposed a 2-level SVD and 2D DWT based video watermarking technique. In this method, the binary watermark was embedded into the sub bands like LL and HL and the author has engaged the dual level SVD for processing. This method was robust against filtering attacks but suffered from frame processing attacks and addition of noise.

Thind and Jindal [15], have proposed a DWT and SVD based video watermarking. In this methodology, the HH sub band was selected for watermark embedding process. The author has combined the DWT and SVD in which the watermark was embedded. In this method, watermark was inserted into every frame of the video wherein the time taken for embedding and extraction process was pretty high.

Rajab et al. [16], proposed a blind of video watermarking technique using DWT-SCHUR. The SCHUR decomposition was performed and DWT was applied in the video scene. The binary image was selected as a watermark which was embedded into the upper portion of HL sub band. This method was unable to resist the frame dropping attack.

Masoumi and Amiri [17], did propose a video copyright protection using scene change analysis. In this method scene change analysis was done and then 3D DWT was applied into the wavelet coefficients. The watermark was inserted into the third level 3D coefficients. Finally, the watermark was embedded into the selected coefficients using spread spectrum concept.

The literature survey revealed the following challenges:

- Since the entire watermark is embedded in all the frames of the video, the embedding and extraction process consumes more time [5, 9, 14–16].
- Identical watermark is embedded in the selected frames which can be easily identified by frame dropping attack [10, 12, 13, 17].
- Methods in which block of watermarks are embedded in the selected frame can withstand frame dropping attack; however these methods [6, 8, 11] are not able to achieve good trade-off between the robustness and imperceptibility.

In order to address the above mentioned challenges and also to withstand various attacks such as frame dropping, frame averaging, frame swapping, filtering and addition of noise, the method proposed in this paper employs Fibonacci based key frame selection and Fibonacci–Lucas Transform based watermark scrambling for embedding watermark in DWT–SVD domain.

The primary contributions of this paper are as follows.

- A method to scramble the watermark using Fibonacci -Lucas transform is proposed to encrypt the watermark.

- A procedure for selecting the keyframes using Fibonacci sequence is proposed, to reduce both embedding and extraction time.
- A procedure for identifying suitable scaling factor is proposed, to have better trade-off between the robustness and imperceptibility.
- A method is proposed to select suitable threshold for identifying the required number of scene changes in the video to embed the watermark with less processing time.

This paper organizes four sections. Section 1 presents the introduction about the scheme and review of literature. Section 2 of this article deals with the proposed methodology which involves scene change detection, DWT, SVD, Fibonacci Lucas transform, watermark embedding and extraction algorithms. In Sect. 3, the results of various experiments along with the comparison of results with existing schemes are highlighted. Finally, in Sect. 4, conclusion is presented.

2 Proposed Methodology

We propose a Fibonacci based key frame selection and scrambling for Video Watermarking in DWT–SVD for protecting video contents against various attacks. The video is processed initially to detect the number of scene changes using the histogram difference method. The R component of the video is selected for embedding process. The watermark data which is to be embedded is scrambled by Fibonacci–Lucas transform which appears like an encrypted watermark. Thereafter it is divided into several sub-watermarks equivalent to the number of keyframes selected in the individual scene. Then the video is subjected to DWT and SVD to embed the sub-watermarks into the LH sub bands of keyframes in the detected scene changes. The proposed methodology is blind because, the watermark can be extracted without the original video. In the absence of original one the resultant system can be utilized for public applications.

2.1 Scene Change Detection

Scene change detection methodology is employed for detecting motion scene in the host video which can be identified by employing histogram difference method. In this method, the difference between the frames is compared with predefined threshold value [18, 19].

The formula for finding the histogram difference is as represented in Eq. 1.

$$hds(f_1, f_2) = \sum_{i=1}^l \frac{(h_i(f_1) - h_i(f_2))^2}{\max(h_i(f_1), h_i(f_2))} \quad (1)$$

where $h(f_1)$ —histogram for frame f_1 with l histogram bins. f_2 —successive frame of f_1 ; hds —histogram difference.

Scene change detection is performed between the consecutive frames based on the histogram differences [18, 19]. The number of scene changes depends on the predefined threshold value. Table 1 shows the variations between the processing time and number of scene changes for specific threshold value. To reduce the computational time and also to improve the security of the watermarking system, a threshold value of 0.25 with 9 scene changes is selected. The threshold value 0.25 is fixed for of all the frames in the video.

Table 1 Number of scene changes based on Threshold value

Threshold	0.1	0.25	0.3	0.35	0.4	0.5	0.65	0.75	0.85	0.95
Number of scene changes	12	9	8	5	5	5	5	3	3	3
Embedding time (s)	16.72	13.21	11.95	10.12	10.12	10.12	10.12	7.26	7.26	7.26

2.2 Discrete Wavelet Transform

The discrete wavelet transform (DWT) splits a video frame into four sub bands such as LL, HL, LH and HH. The wavelet basis function is represented in Eq. 2 [20]. Here the 2D wavelet transform is used to split the video frames into sub bands as shown in Fig. 1a.

$$\phi(X) = \sum_{j=0}^{M-1} C_j \phi(2X - j) \tag{2}$$

where M is the number of non-zero coefficients. $\phi(2X - j)$ is the scaling function. j is the scaling index.

Experiments have been conducted using various 2D wavelets such as Haar, Db2, Db4 and Db6 etc., Based on literature survey and the performance derived from such experiments, it is found that Haar wavelet is suitable for embedding watermark.

The Haar wavelet is a square shaped function which is simple and easy for implementation. It is characterized by its orthogonal property and it entails good performance in terms of computation [21].

The Haar wavelet is represented in Fig. 1b.

Single level discrete wavelet transform decomposes the image into one approximation subband LL and three detailed subbands namely LH, HL and HH. Embedding watermark in the higher frequency subband (HH) increases its robustness at the cost of the image

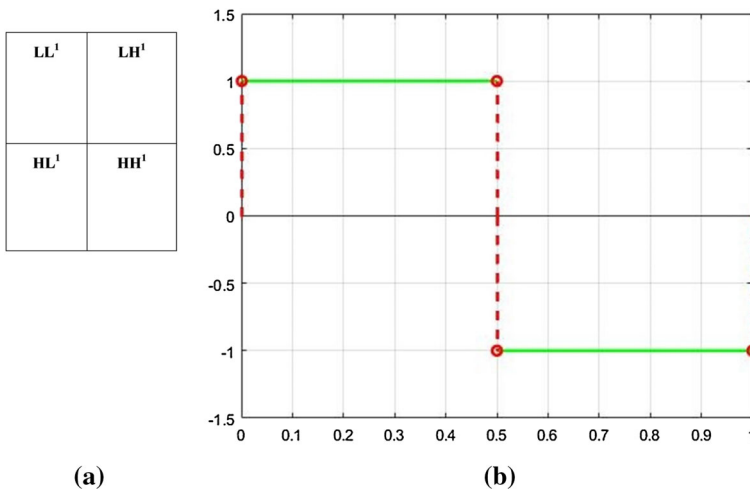


Fig. 1 a One level DWT and b Haar wavelet transform

visual fidelity. Experiments have been conducted to identify the suitable subband and the number of levels of DWT decomposition required to embed the watermark with good trade-off between the robustness of the watermark and image visual quality. In order to measure the robustness and visual quality the metrics NCC and PSNR are used respectively. The results are presented in Table 2.

It is quite evident from the table that the PSNR and NCC value of LH and HL is better than the other two subbands (LL and HH). Among LH and HL subbands, the LH subband provides better performance in terms of both PSNR and NCC.

It can also be observed from the Table 2 that increasing the level of decomposition after first level are not producing good perceptual quality and robustness in terms of PSNR and NCC respectively. Hence the proposed approach applies single level of decomposition and LH subband for embedding the watermark.

2.3 Fibonacci Sequence

Fibonacci numbers are the sequence of values that are generated using a fixed pattern.

The Fibonacci sequence is defined by the recurrence relation as represented in Eq. 3.

$$f_N = f_{N-1} + f_{N-2} \tag{3}$$

The initial seeds are $f_0 = 0$ and $f_1 = 1$.

This Fibonacci sequence is used to select the keyframes in the entire scene of the video.

2.4 Fibonacci Lucas Transform

The secret image is scrambled using Fibonacci–Lucas transform. The Lucas transform is represented in Eq. 4.

$$L_N = \begin{cases} 2, & \text{if } N = 1 \\ 1, & \text{if } N = 2 \\ L_{N-1} + L_{N-2} & \text{otherwise} \end{cases} \tag{4}$$

Here $L_1 = 1$ and $L_2 = 2$ are initial values of the sequence. The subsequent values are derived from these initial values as defined by the expression, $L_N = L_{-1} + L_{-2}$.

For example when $N = 3$, $L_3 = L_2 + L_1$.

Here $L_1 = 2$; $L_2 = 1$, Hence $L_3 = 3$.

Hence the L_N sequence will be 2, 1, 3, 4, 7, 11, 18, and 29.

Table 2 PSNR of watermarked video and NCC of extracted watermark for various subbands

Level of DWT	LL		HH		HL		LH	
	PSNR (dB)	NCC	PSNR (dB)	NCC	PSNR (dB)	NCC	PSNR (dB)	NCC
First level	39.54	0.76	50.27	0.81	51.28	0.93	53.34	0.99
Second level	34.65	0.74	47.92	0.79	48.19	0.88	50.12	0.90
Third level	30.58	0.69	42.35	0.75	46.24	0.81	47.83	0.87

Lucas series do not have a uni-modular periodic property. In order to achieve this, Lucas transform is combined with Fibonacci to form the Fibonacci–Lucas transform [20, 22]. It is represented in Eq. 5.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{M} \tag{5}$$

where $x, y \in \{0, 1, 2, \dots, N - 1\}$, F_n is the n th term of the Fibonacci series and L_n is the n th term of the Lucas series, ($n = 1, 2, \dots$ except for $n = 3$). M is the size of the secret image, that is $M = \text{Height} * \text{Width}$.

The first 15 values of Fibonacci and Lucas series are represented in Table 3.

F_{12_n} -Fibonacci sequence, L_n -Lucas sequence, F_{31_n} -Fibonacci–Lucas sequence.

For each value of i , the Fibonacci–Lucas transform attain maximum periodicity, so that the image information can be redistributed uniformly across the scrambled image. The sample scrambled images namely Lena, trees, penguin, which are represented in the Fig. 2. It is evident from the Fig. 2 that the quality of the scrambled image appears to be good enough in all the images.

2.5 Watermark Pre-process

The Watermark should be a binary image. It is scaled to specific size by Eq. 6.

$$2^e \leq g, e > 0 \tag{6}$$

The selected watermark is permuted based on Fibonacci–Lucas transform to produce scrambled watermark, which looks like encrypted watermark.

Where g is the number of scene changes in the video, e is the integer.

Scrambled watermark is divided into 2^e small independent watermark blocks. These two blocks are equivalent to number of keyframes selected for each scene which are represented in the embedding key generation Table 4.

2.6 Diffie–Helman Key Exchange Algorithm

In the proposed approach, two different secret keys are generated for the purpose of improving the authentication of the host video and secret image. The first authentication keys are generated by Fibonacci sequence for embedding the secret image in the specific keyframe which is represented in Table 4. The second secret keys are generated by using Fibonacci–Lucas transform for scrambling the secret image. These two sets of keys are generated by sender. Secret keys are necessary, if receiver wants to extract the watermark means. For this purpose, the Diffie–Helman key exchange algorithm is used. These two

Table 3 Fibonacci and Lucas series

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_{12_n}	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987
L_n	2	1	3	4	7	11	18	29	47	76	123	199	322	521	843
F_{31_n}	3	1	4	5	9	14	23	37	60	97	157	254	411	665	1076

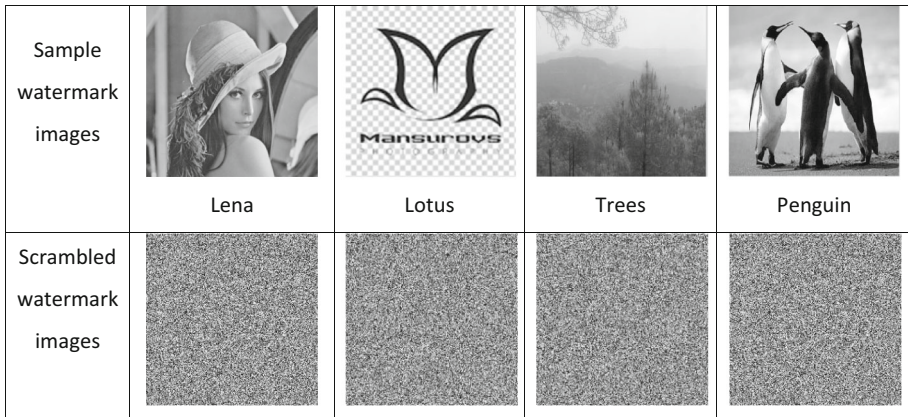


Fig. 2 Sample and scrambled images

Table 4 Embedding key generation

Changed scene number (CS)	Initial key value (K1, K2)	Key frame 1	Key frame 2	Key frame 3	Key frame 4	Key frame 5	Key frame 6	Key frame 7	Key frame 8
103	10, 3	10	3	13	16	29	45	74	
117	104, 14	118	132						
133	118, 16	134							
147	134, 14	148	162						
163	148, 16	164	180	196					
209	164, 46	210							
255	210, 46	256							
271	256, 16	272	288	304	320	336	352	368	384

keys are securely sent by this method. It is a public key cryptographic system which is applicable to N number of receivers [23–25].

2.7 Watermark Embedding Process

In embedding process, the RGB frame is split it into R, G and B channels. Since R component is a better match with human visual system (HVS) and gives effective robustness, the R component of the video is selected for embedding process [17]. The scrambled watermarks are split into various blocks based on available keyframes in the scene. The scrambled blocks are embedded into the appropriate keyframes in each scene of the source video. The keyframes are identified by using Fibonacci sequence. Here Suzie video is taken as host video which contains 451 frames with the RGB format. The key-frame selection procedure is represented in Table 4. The First initial key values are selected from the frame number of the first scene change. Other initial key values are selected based on the key frame generation rule. The watermark embedding process is represented in Fig. 3.

Rule for key Generation

```

Number of keyframe=Number of Changed scene
First scene change=Generate key frames based on Fibonacci
Sequence
Key1: Previous scene number (CS) +1
Key2: Difference between the succeeding scenes
Key frame=K1+K2
    K1=Current key frame;
    K2=K2;
    If keyframe_number >Succeeding Scene number
        Stop the process
    Else
        Generate key frames using K1 & K2

```

Watermark embedding algorithm

Input: Host Video and Binary image

Output: Watermarked Video

Prior process:

- Input Video (A) is pre-processed and fragmented into number of frames. The Red component is only taken for the embedding process.
- Obtain number of scenes (N) by applying scene change detection into original video. Select each scene and do:

Step 1: In Each scene identify the keyframes for embedding the scrambled watermark block.

Step 2: Apply 2D Wavelet transform to each scene to produce sub bands HH, HL, LH, LL.

Step 3: Sub band LH is selected and subjected to SVD transformation.

$$X_s = U_a S_a V_a^T$$

Step 4: Scrambled the watermark image (W) and partition into number of blocks (n) $W_{b1}, W_{b2}, \dots, W_{bn}$, $n = N$, Number of block is equivalent to number of keyframes.

Step 5: Apply SVD transformation to each scrambled W_b block

$$W_b = U_w S_w V_w^T$$

Step 6: Watermark transformed block (S_b) is added to the singular values (S_a) of the scene S.

$$S_n = S_a + kS_w$$

k is the scaling factor; it depends on the watermark image.

Step 7: Perform inverse SVD on S_n to get watermarked scenes.

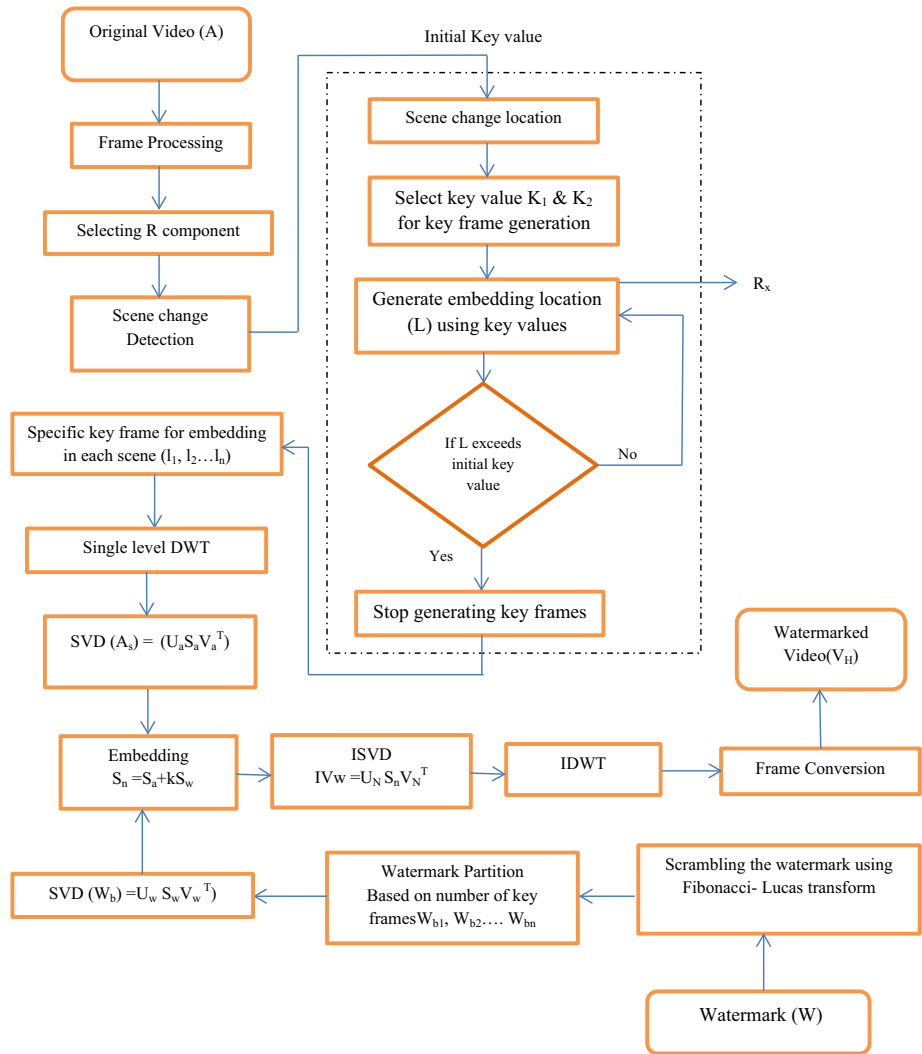


Fig. 3 Watermark embedding process

$$IVw = U_N S_n V_N^T$$

Step 8: Combine all scenes and Perform Inverse DWT (IDWT), which is used to reconstruct the video from the modified levels and also perform frame conversion to get Watermarked Video (V_H). The output produced by the inverse DWT is same as the input of the forward DWT.

The scaling factor is used to control both perceptual quality and robustness of the embedding process. Experiments have been conducted for different scaling values. Based on the robustness of the watermarked video and perceptual quality of the watermark, the appropriate scaling factor is selected. The perceptual quality and the robustness are measured by the metrics PSNR and NCC respectively. The trade-off between the PSNR

and NCC is used for selecting the suitable scaling factor. The variations of PSNR and NCC for different scaling factors are shown in Table 5.

It is observed from the table that the scaling factor of 0.25 shows better trade-off between PSNR and NCC value. After 0.25 the NCC value increases but the PSNR value drastically decreases. Hence the scaling factor 0.25 is selected for processing of watermark.

2.8 Watermark Extraction

To extract watermark, SVD is applied on the watermarked video and the watermarked matrix is computed. From this matrix, the watermark is extracted using the scaling factor k . The value of k depends on the secret image. The watermark extraction process is presented in Fig. 4. From the watermarked video, the watermark is extracted using the same process as followed in embedding. The scene change detection is performed and thereafter R component is selected for further process. The DWT and SVD are applied for transformation. The embedded keyframe location is identified for extraction process and then the scrambled watermark block is extracted from the individual keyframes in each scene. Then the watermark block are combined to obtain complete scrambled watermark followed by application of Fibonacci–Lucas sequence to transform the scrambled watermark into original watermark.

Watermark extraction algorithm

Input: Watermarked Video
 Output: Extracted Watermark

Prior process:

- Watermarked Video (V_H) is processed and fragmented into number of frames. The Red component is selected for further processing.
- Applying scene change detection into Watermarked Video in order to identify various scenes.

Select each scene and do

Step 1: Each scene is subjected to 2D wavelet transform, it produce four sub bands Such as LL, HL, LH, HH.

Step 2: Identify the keyframes for each scene.
 Sub band LH is subject to SVD transformation to obtain watermarked matrix (S_H)

$$L_w = U_H S_H V_H$$

Step 3: Extract scrambled watermark block from each scene.

$$W'_b = (S_H - S)/k$$

Table 5 Selection of scaling factor based on PSNR and NCC

Scaling factor	0.1	0.15	0.25	0.35	0.45	0.55	0.65	0.75	0.85
PSNR	55.61	54.01	53.34	50.12	47.23	40.17	38.71	35.24	33.21
NCC	0.95	0.96	0.98	0.98	0.99	0.99	1	1	1

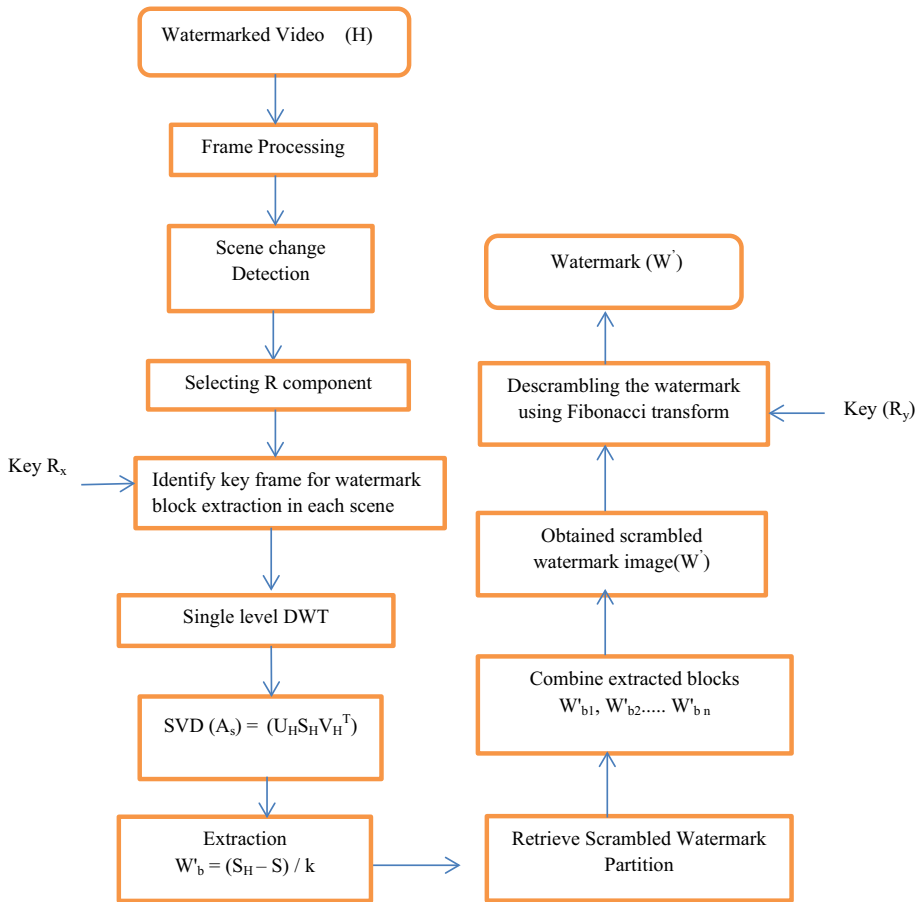


Fig. 4 Watermark extraction process

- Step 4: Combine all the extracted block ($W'_{b1}, W'_{b2}, \dots, W'_{bn}$) to obtain whole scrambled Watermark W' .
- Step 5: Watermark W' is subjected to Fibonacci–Lucas transformation for converting the scrambled watermark to original watermark image (W).

3 Results and Discussion

Experiments are conducted for assessing the proposed Fibonacci based keyframe selection and scrambling for Video Watermarking in DWT–SVD. The chosen input video sequences (Suzie, Foreman and News) in the RGB, AVI format with frame rate of 30 frames/sec are available in the standard library. The experiment was done in WINDOWS platform with i3 processor using MATLAB 2011.

The snapshots from these videos are shown in the Fig. 5. Scene changes in the original video are identified from the histogram difference which is greater than the threshold. The

histogram difference between neighbouring frames of the host video Suzie is depicted in Fig. 6.

Binary images are used as watermarks; their resolution depends on the resolution of the initial video. The watermark logo, the watermarked video and the extracted watermark are shown in Fig. 7.

3.1 Assessment of Robustness

The robustness of proposed watermarking algorithm is evaluated by conducting several experiments using MATLAB 2011. Various image and video processing attacks like filtering, addition of noise, compression, blur, brighten, frame averaging, frame swapping and frame dropping were applied on the watermarked video. The quality of the watermarked video is evaluated in terms of the mean PSNR (peak signal to noise ratio) value, Normalised cross correlation (NCC) and Bit Error Rate (BER), which are represented in Eqs. 7, 8 and 9 respectively. NCC measures the difference between the extracted watermark and the original watermark.

$$PSNR(I, \hat{I}) = 10 \text{Log}_{10} \frac{255^2}{\frac{1}{LK} \sum_{i=1}^L \sum_{j=1}^k \left(I_{ij} - \hat{I}_{ij} \right)^2} \quad (7)$$

$$NCC = \frac{\sum_i \sum_j W(i,j) \cdot \hat{W}(i \cdot j)}{\sum_i \sum_j [W(i,j)]^2} \quad (8)$$

$$BER \left(W, \hat{W} \right) = \frac{1}{P} \sum_{j=1}^P \left| \hat{W}(j) - W(j) \right| \quad (9)$$

Frame dropping attack: Particular frames are removed from the watermarked video which is called frame dropping. In this attack, 25% of the watermarked video frames are got dropped.

Frame averaging attack: The current frame is replaced by the average of the current frame and its two nearest neighbours. It is made on 25% of the watermarked video frame.

Frame swapping attack: It is applied by swapping the current frame and the frame just ahead of it. This attack is also performed against 25% of the watermarked video frame.

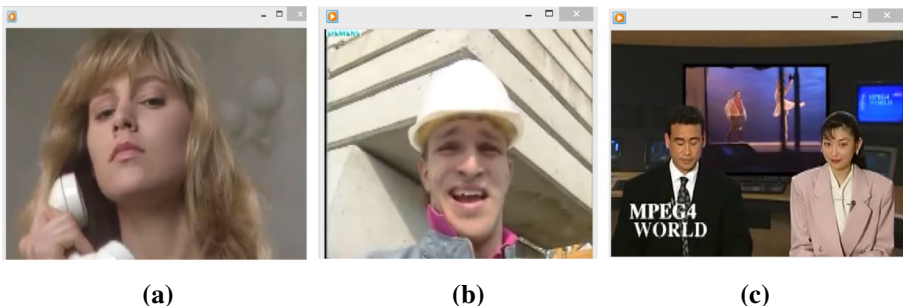


Fig. 5 Snap shots of original video. **a** Suzie, **b** Foreman and **c** News

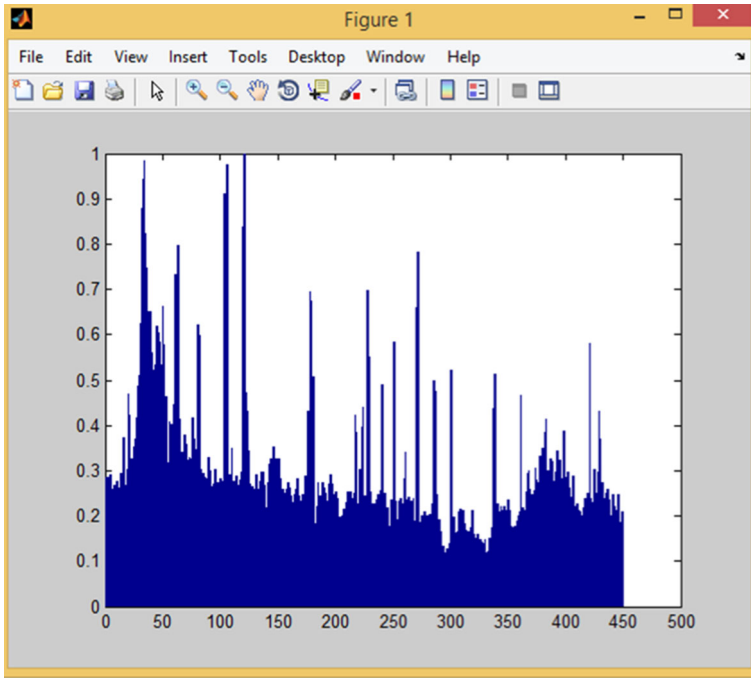


Fig. 6 Scene change detection using histogram difference method

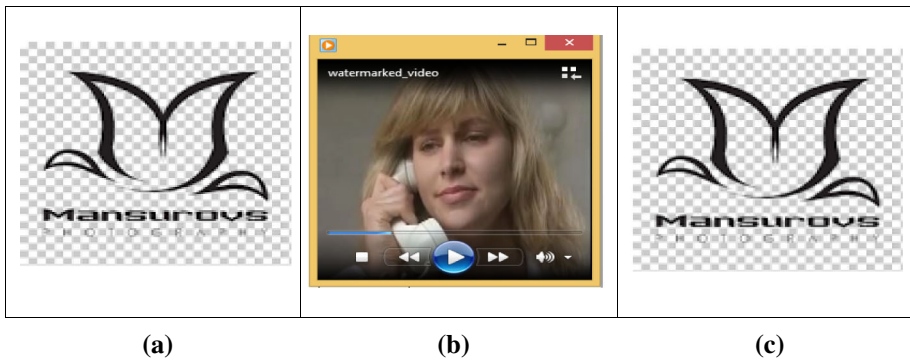


Fig. 7 **a** Watermark logo, **b** sample watermarked video and **c** extracted watermark

Addition of noise: Addition of noise normally results in the alteration and degradation of the video. Different kinds of noise such as Gaussian, salt and pepper and Poisson noise with 10% variance and zero mean are added to the output video.

The PSNR value of the attacked video was found to be 48.96 dB, 46.54 dB and 55.28 dB with Gaussian noise, salt and pepper noise and Poisson noise, respectively.

After applying various kinds of attacks, the watermarked video quality is significantly reduced and fewer amounts of data are lost. Hence the watermark image is detectable with acceptable PSNR and NC values.

The resulting PSNR values of various watermark lies between 62.7 and 57.5 dB and the watermarked videos appear visually match with the original video. The PSNR value which is obtained for the video Suzie works out to 53.34. Extracted watermark has the PSNR value of 62.3. The PSNR values of different watermarks embedded in the original video are presented in the Table 6.

The snapshot of the attacked watermarked video and the corresponding PSNR values are shown in the Table 7.

Various attacks were carried out on the watermarked video and then the watermark is extracted after each attack. The PSNR values of the extracted watermark were computed and compared with the various existing algorithms. Figure 8 shows the PSNR values of watermark extracted from the video after various attacks. The recovered watermark is found to be identical to the original. Hence the proposed algorithm is robust against various attacks like blurring, brighten, adding Gaussian, salt & pepper, Poisson noise, frame averaging and frame swapping.

3.2 Result Comparisons with Existing Algorithms

The PSNR value of the video obtained from the proposed algorithm is compared with the existing algorithm which is shown in Table 8.

In human perception, PSNR value of 40 dB and higher is believed to be better value [26]. It can be seen from the Table 8 that the proposed approach provides PSNR value from 41.13 to 52.12 dB under various attacks, which are better than the other existing methods. Under no attack condition the proposed approach provides PSNR value of 53.34 dB which is better than the existing methods other than the method by Thind and Jindal [15]. However the method suggested by Divjot Kaur et al. miserably fails under various attacks compared to the proposed method. This is because Divjot Kaur et al. have embedded the whole watermark into every frame of the video. Whereas in the proposed approach, blocks of watermark was embedded into the different key frames. Hence the proposed method provides better PSNR than Divjot Kaur et al. method under various attacks.

Table 6 PSNR values of different watermarks embedded in the original video





Watermarks				
PSNR (dB)	62.3	60.5	57.5	61.7

Table 7 Watermarked video after applying various attacks with PSNR value

Attack type	No attack	Gaussian Noise	Poisson Noise	Salt and pepper Noise
Output Video				
PSNR (dB)	53.34	47.96	47.82	45.45
Attack type	Blur	Frame Dropping	Frame averaging	Frame Swapping
Output Video				
PSNR (dB)	51.83	52.34	43.39	52.17

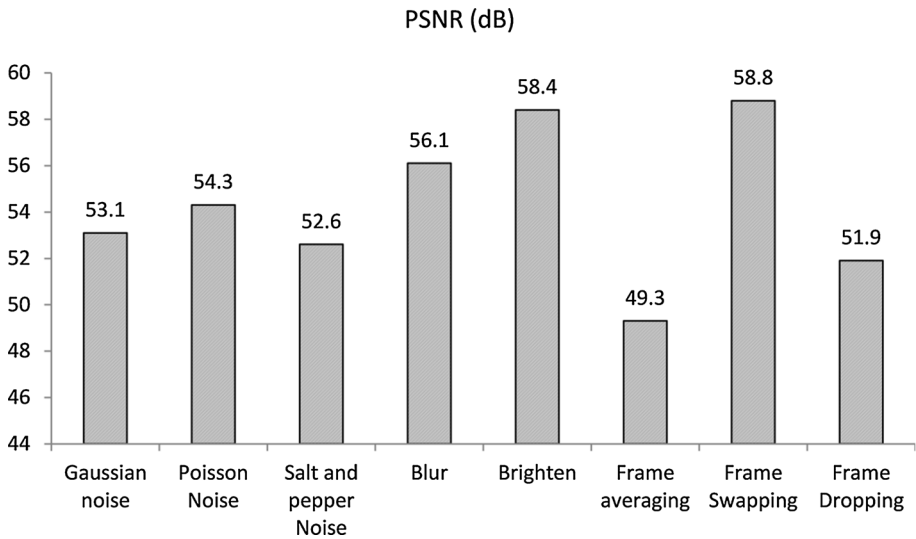


Fig. 8 PSNR values of watermark extracted from the video after various attacks

Table 8 Comparison of PSNR values of watermarked video in dB compared with various existing methodology

Name of the attack	Preda et al. [12]	Thind et al. [15]	Faragallah [13]	Preda et al. [10]	Proposed method
No attack	38.30	63.7	44.83	48.91	53.34
Blur	32.80	36.8	33.42	33.43	51.83
Brighten	30.50	30.91	32.48	32.74	52.12
Gaussian	33.49	33.29	36.69	32.91	47.96
Median	27.41	27.51	27.48	27.41	41.13
Salt and pepper	30.03	32.30	34.33	38.19	45.45
Frame average	36.80	38.50	44.85	47.00	48.39
Poisson	30.21	35.62	39.27	40.22	47.82

The Normalised cross correlation values between the extracted watermark and the original watermark are obtained after applying various attacks in the watermarked video which can be compared with various existing methods as shown in Fig. 9.

To evaluate the performance, the result of the proposed methodology is compared with different available schemes. The PSNR metric is compared with the existing method delivered by Preda and Vizireanu [10], Preda and Vizireanu [12], Faragallah [13] and Thind and Jindal [15]. The proposed method generates better PSNR values for median filtering and addition of noise and frame averaging.

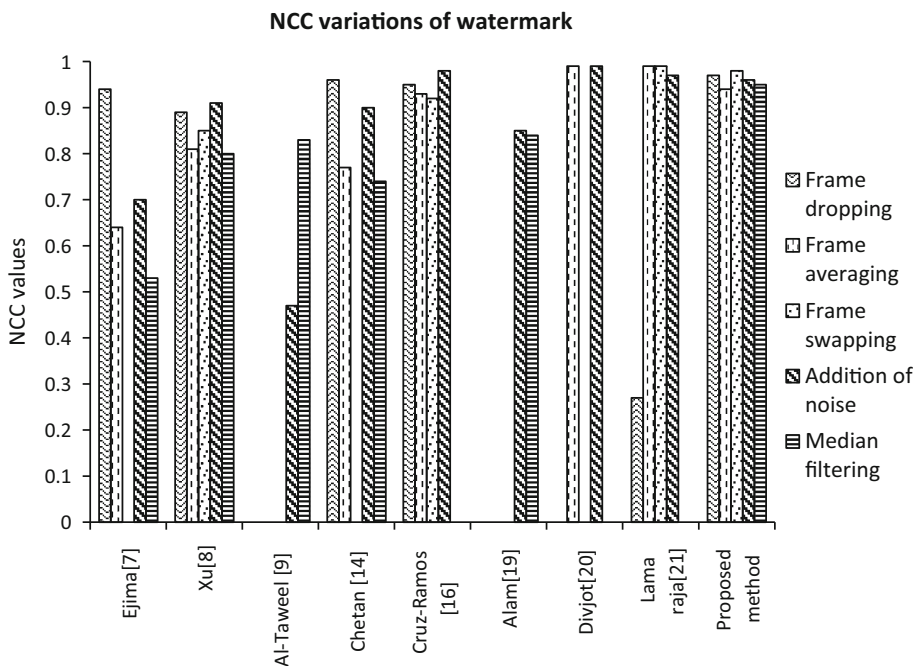


Fig. 9 NCC variations of watermark in various attacks compared with exiting methodology

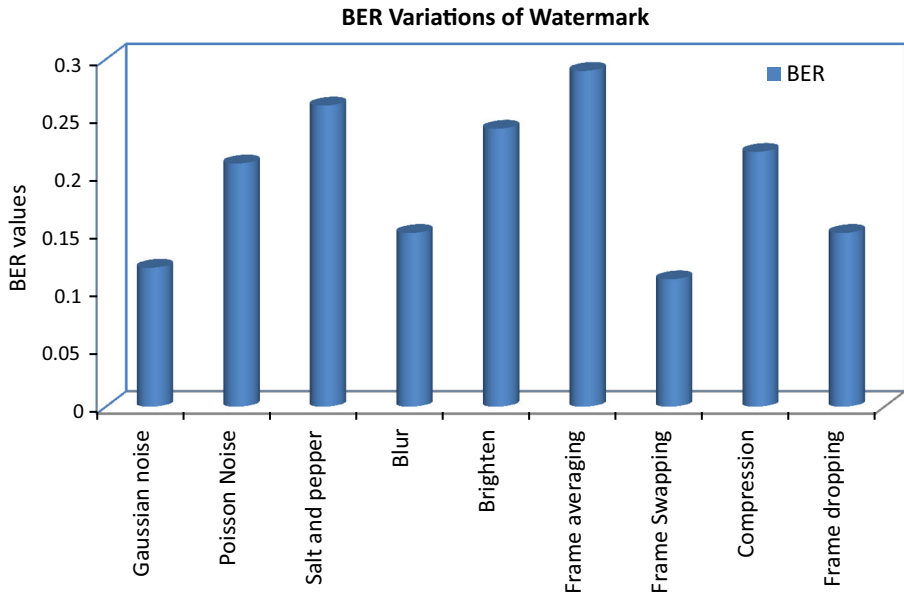


Fig. 10 BER variations of watermark in various attacks for proposed methodology

The BER values are calculated between the original and extracted watermark as shown in the Fig. 10. The BER values of the watermark for various attacks are less than 0.3, which shows that the proposed algorithm improves the imperceptibility of the watermark.

The NCC values of extracted watermark are compared with the various existing methodology delivered by Ejima and Miyazaki [5], Xu [6], Al-Taweel and Sumari [7], Chetan and Raghavendra [9], Cruz-Ramos et al. [11], Alam Naved and Yadav Rajesh [14], Thind and Jindal [15] and Rajab et al. [16]. The NCC values of the proposed algorithm are comparatively higher than the existing methodology for various kinds of attacks like blur, brighten, addition of noise, filtering, frame dropping and averaging. This algorithm is experimented for various input videos like Suzie, Foreman and News, with different attacks. The resultant PSNR values are consistent in different inputs as shown in Fig. 11. This proves the quality of the proposed methodology.

4 Conclusion

In this paper, Fibonacci based keyframe selection and scrambling for Video Watermarking in DWT–SVD is proposed. The watermark embedding process is applied in the coefficients of LH sub band. For improving the robustness and imperceptibility of the host video and secret image, two different transformations like DWT and SVD are combined and used. To improve the video authenticity, the keyframe selection concept is introduced where the watermark got scrambled using Fibonacci–Lucas transform. For the purpose of reducing the time complexity of the process, the watermark is selectively embedded in the changed scene. The watermark is divided into number of blocks and embedded into the keyframes with a view to reducing the frame dropping attack. The secret keys of the embedding

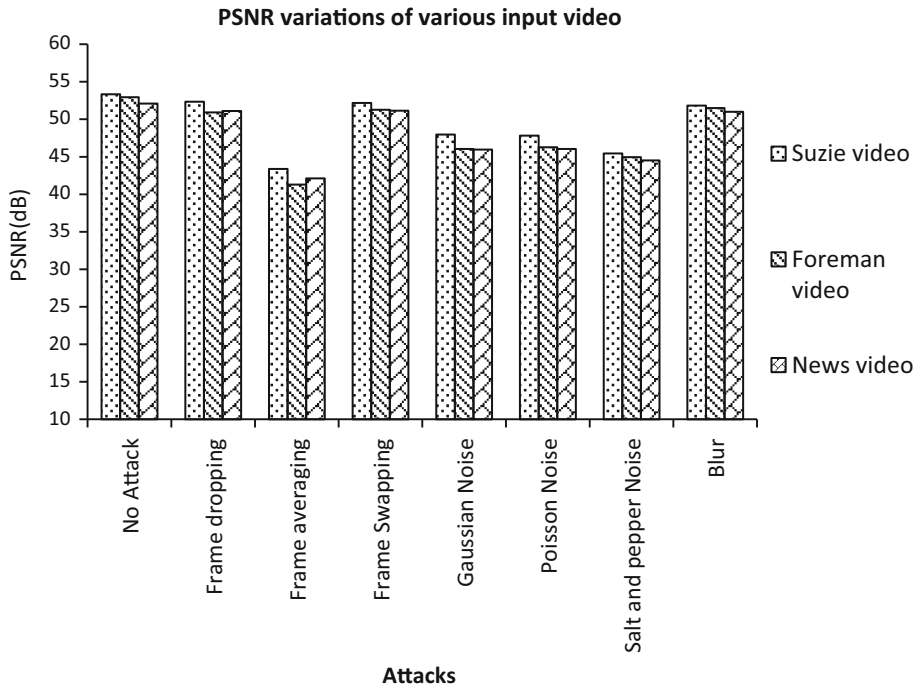


Fig. 11 PSNR variations of various input video

location and watermark scrambling keys are securely sent to the receiver by Diffie-Helman Key exchange Algorithm. It enhances the authentication of the video as well as secret image. From the experimental results, it is quite evident that the proposed algorithm with stand various attacks with better performance.

References

1. Langelaar, G. C., Setyawan, I., & Legendijk, R. L. (2000). Watermarking digital image and video data. A state-of-the-art overview. *IEEE Signal Processing Magazine*, 17(5), 20–46.
2. Chang, X., Wang, W., Zhao, J., & Zhang, L. (2011). A survey of digital video watermarking. In *2011 Seventh international conference on natural computation (ICNC)* (Vol. 1, pp. 61–65). IEEE.
3. Paul, R. T. (2011). Review of robust video watermarking techniques. *IJCA Special Issue on Computational Science*, 3, 90–95.
4. Hernandez-Guzman, V., Cruz-Ramos, C., Nakano-Miyatake, M., & Perez-Meana, H. (2006). Watermarking algorithm based on the DWT. *IEEE Latin America Transactions*, 4(4), 257–267.
5. Ejima, M., & Miyazaki, A. (2000). A wavelet-based watermarking for digital images and video. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 83(3), 532–540.
6. Xu, D. W. (2007). A blind video watermarking algorithm based on 3D wavelet transform. In *2007 International conference on computational intelligence and security* (pp. 945–949). IEEE.
7. Al-Taweel, S. A., & Sumari, P. (2009). Robust video watermarking based on 3D-DWT domain. In *TENCON 2009–2009 IEEE region 10 conference* (pp. 1–6). IEEE.
8. Reyes, R., Cruz, C., Nakano-Miyatake, M., & Perez-Meana, H. (2010). Digital video watermarking in DWT domain using chaotic mixtures. *IEEE Latin America Transactions*, 8(3), 304–310.

9. Chetan, K. R., & Raghavendra, K. (2010). DWT based blind digital video watermarking scheme for video authentication. *International Journal of Computer Applications*, 4(10), 19–26.
10. Preda, R. O., & Vizireanu, D. N. (2010). A robust digital watermarking scheme for video copyright protection in the wavelet domain. *Measurement*, 43(10), 1720–1726.
11. Cruz-Ramos, C., Reyes-Reyes, R., Nakano-Miyatake, M., & Pérez-Meana, H. (2010). A blind video watermarking scheme robust to frame attacks combined with MPEG2 compression. *Journal of Applied Research and Technology*, 8(3), 323–337.
12. Preda, R. O., & Vizireanu, D. N. (2011). Robust wavelet-based video watermarking scheme for copyright protection using the human visual system. *Journal of Electronic Imaging*, 20(1), 013022.
13. Faragallah, O. S. (2013). Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. *AEU-International Journal of Electronics and Communications*, 67(3), 189–196.
14. Naved, A., Rajesh, Y. (2013). Dual band watermarking using 2-D DWT and 2-level SVD for robust watermarking. In *Video. International Journal of Science and Research (IJSR)*, India Online ISSN: 2319-7064.
15. Thind, D. K., & Jindal, S. (2015). A semi blind DWT–SVD video watermarking. *Procedia Computer Science*, 46, 1661–1667.
16. Rajab, L., Al-Khatib, T., & Al-Haj, A. (2015). A blind DWT-SCHUR based digital video watermarking technique. *Journal of Software Engineering and Applications*, 8(04), 224–233.
17. Masoumi, M., & Amiri, S. (2013). A blind scene-based watermarking for video copyright protection. *AEU-International Journal of Electronics and Communications*, 67(6), 528–535.
18. Zong, T., Xiang, Y., Natgunanathan, I., Guo, S., Zhou, W., & Beliakov, G. (2015). Robust histogram shape-based method for image watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*, 25(5), 717–729.
19. Singh, T. R., Singh, K. M., & Roy, S. (2013). Video watermarking scheme based on visual cryptography and scene change detection. *AEU-International Journal of Electronics and Communications*, 67(8), 645–665.
20. Mishra, M., Mishra, P., Adhikary, M. C., & Kumar, S. (2012). Image encryption using Fibonacci–Lucas transformation. *International Journal of Cryptography and Network Security*, 2, 131–141.
21. Mallat, S. (1999). *A wavelet tour of signal processing*. Cambridge: Academic press.
22. Zou, J., Ward, R. K., & Qi, D. (2004). The generalized Fibonacci transformations and application to image scrambling. In *IEEE international conference on acoustics, speech, and signal processing, 2004. Proceedings. (ICASSP'04)* (Vol. 3, pp. iii–385). IEEE.
23. Diffie, W., Van Oorschot, P. C., & Wiener, M. J. (1992). Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2), 107–125.
24. Burmester, M., & Desmedt, Y. (2005). A secure and scalable group key exchange system. *Information Processing Letters*, 94(3), 137–143.
25. Lu, R., & Cao, Z. (2007). Simple three-party key exchange protocol. *Computers & Security*, 26(1), 94–97.
26. Bull, D. R. (2014). *Communicating pictures: A course in image and video coding*. Cambridge: Academic Press.



S. Ponni alias Sathya received B.E. degree in computer Science and Engineering in 2004 from the Madurai Kamaraj University, Madurai and M.E., degree in Computer Science Engineering in 2009 from Anna university, Chennai. She has 10 years of teaching experience. She is working as Assistant professor of Information Technology at Dr. Mahalingam College of Engineering and Technology, Pollachi, India. Her research interest covers video processing, image encryption, multimedia data security.



Dr. S. Ramakrishnan received the B.E. (ECE) in 1998, a M.E. (CS) in 2000 and PhD degree in Information and Communication Engineering from Anna University, Chennai in 2007. He is a Professor and the Head of IT Department, Dr. Mahalingam College of Engineering and Technology, Pollachi. He has 17 years of teaching experience and 1 year industry experience. He has published 152 papers and 8 books. He is an Associate Editor for IEEE Access and he is a Reviewer of 25 International Journals including 7 IEEE Transactions, 5 Elsevier Science Journals, 3 IET Journals, ACM Computing Reviews, Springer Journals, Wiley Journals, etc. He is in the editorial board of 7 International Journals. He is a Guest Editor of special issues in 3 International Journals including Telecommunication Systems Journal of Springer. His areas of research include digital image processing, information security, and soft computing.