Received: August 10, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Robust Video Watermarking Using Secret Sharing, SVD, DWT and Chaotic Firefly Algorithm

Bhargavi Latha S[1]* **Venkata Reddy Dasari[2]** **Damodaram Avula[3]**

[1]*Department of Computer Science and Engineering,*
Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India
[2]*Department of Electronics and Communication Engineering,*
Mahatma Gandhi Institute of Technology, Hyderabad, India
[3]*Department of Computer Science and Engineering, Sri Venkateswara University, Tirupathi, India*
* Corresponding author's Email: s.bhargavilatha@gmail.com

Abstract: Watermarking is the process to protect and discourage the illegal sharing of multimedia content through digital data sharing websites over INTERNET and also to prove ownership of the multimedia content. Though various watermarking solutions are available to safeguard the digital media, at the same time many methods exist to weaken the strength of watermark hence ownership is disproved and can be shared illegally. Strength of watermark can be increased to make it to robust against these methods at the cost of perceptual quality. So, a compromised approach is required. This paper proposes a video watermarking solution to maintain robustness as well perceptual quality through optimization. This method adds secretly shared watermark bits to singular values of the discrete wavelet coefficients with proper scaling factor, which is selected by using the Chaotic Firefly Algorithm optimization method. Despite many watermarking methods exist on combination of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), these are not effective against all filtering attacks as these are not using all frequency coefficients either for embedding or secret sharing. This method generates secretly shared watermark based on singular values in DWT domain to make the system more robust against filtering attacks and video compression techniques. This solution leverages chaotic firefly algorithm to compromise robustness and perceptual quality of the input along with SVD and DWT. The performance of method is measured by evaluating it on a dataset comprised of 140 videos of various genre and compared its performance with state of art methods. Eventually, proved the method is performing well when compared to state of art methods with respect to robustness as well as quality at the cost of computation. The stated results in experimental section shows us that watermark can be retrieved even if watermarked audio undergoes several attacks like compression at lower bit rates, frame drop attack and resize attack etc.

Keywords: Singular value, Wavelet-transform, Watermark, Video-watermark, Attacks, Chaotic firefly, Optimisation.

1. Introduction

In day to day life, INTERNET becomes the most prominent channel to share the multimedia content. This opportunity brings the both pros and cons to the digital media industry. Positive side of this increases the revenue of the company. In contrast, unfair distribution can be termed as infringement of the multimedia data over INTERNET brings huge loss to the company, multimedia data could be an audio, an image or a videos etc. These cons attracted lot of researchers to find different ways to mitigate this and came up with a solution called watermarking a data before actual distribution.

In watermarking, ownership information is inserted into the multimedia content as a watermark and then retrieved it when necessary to prove its ownership. But watermark can be removed by using signal processing operations generally called as attack, when watermark is inserted using simple watermarking methods. Therefore, a watermarking method should be robust enough against attacks like

filtering, scaling, cropping, rotation, or frame dropping, etc. while maintaining the acceptable signal quality. In this paper we propose a robust method to watermark a video and maintain its signal quality with the help of optimization methods.

Many video watermarking techniques exist with various design trade-offs with the aim that watermark should sustain even when watermarked data is manipulated using various signal processing operations such as filtering, scaling, cropping etc.., without changing signal characteristics of the host video signal. Having said that several methods exist in the current market , which uses Discrete wavelet transform(DWT) [1], singular value decomposition(SVD) [2] because of its advantages like compacts the maximum energy of the signal in a few singular value coefficients by optimal matrix decomposition [3] and also small distortion over the image will not perturb the singular values significantly. This property brings application of the

SVD into image watermarking applications and for the same we have also adopted SVD to video watermarking method proposed in our approach and adopted choatic firefly algorithm to find a scaling factor which maintains robustness and signal quality.

2. Related work

Although, multiple works on DWT for video watermarking exist, each method had its own advantages and disadvantages. Few methods which used DWT for watermarking are Hongmei Liu [4] embedded the watermark directly to the DWT coefficients of LL band of three level DWT, in addition this method used the BCH error correcting codes and also applied 3-D interleaving in order to reduce burst errors. This method may fail against high pass filtering since watermark was inserted in low frequency LL band. Modifying least significant bits of DWT coefficients makes system less robustness against filtering attacks such as sharpening and Gaussian filtering. Rathore[5] followed the same approach by changing scrambling method. H. Tian [6] applied 1D wavelet transform on two consecutive frames, then low frequency part was partitioned into equal size blocks to embed watermark bit based on average pixel value of the block and then same procedure was employed to detect the watermark. Based on published results this method worked well for various compression ratios of mpeg compression, Gaussian noise but will not work against frame drop attack as watermark bit was embedded using two consecutive frames in DWT domain. CE Want [7] embedded two zero mean normally distributed watermarks in Temporal Wavelet Transform (TWT) domain to avoid block effects. This method inserted watermark bit into one block of 32 frames in TWT domain. Watermark extraction becomes challenging against frame drop attacks. Few more approaches used DWT along with other transforms, Method in [8] used both DWT and SVD on both input video frame and input watermark. This method requires to store U and V components of watermark to retrieve the watermark during watermark extraction and it is possible to retrieve watermark by keeping other's watermark S component with existing U and V components, this in turn causes false positives.

Allali [9] employed a watermarking scheme based on Walsh Hadamard Transform (WHT) and DWT, where each video frame was segmented into cubes, DWT is applied followed by 3-level WHT on each row to embed watermark bit to high frequency coefficients. Watermark was retrieved by using the prediction method as specified in [10] and used Wiener filtering. But not evaluated against frame drop attack as well as video compression techniques like x264 etc. Some more methods adopted combination of more than two signal processing techniques like DWT, DCT and SVD in [10] for watermarking the ultrasound signal, watermark was inserted into SVD coefficients of ultrasound in DWT and DCT domain. This paper also employed SVD to watermark due to its characteristics. A concept called Binary Particle Swarm Optimization (BPSO) used [11] to know which frames are suitable for watermarking based on fitness value computed from each frame, the drawback of this method is, it should store list of frame numbers to retrieve the watermark. Other transform like contourlet transform was used in [12] along with discrete wavelet transform and singular value decomposition to watermark a given video and log polar transform was used during extraction of watermark in order to resist geometric attack. Li [13] proposed a method which used discrete cosine transform in order to select low frequency coefficients to embed a watermark and also logistic chaotic map and error-correction coding were adopted to make system robust against attacks. A method [14] developed a watermarking system which used singular value decomposition to insert watermark and also exploited the mosaic from all video frames to insert a double signature in order to improve embedding capacity. Sundararajan [15] inserted watermark in a video by partitioning it into number of frames, then watermark image was sliced into bit planes and permuted them in order to embed into the segmented shot, but this method fail against crop attack.

Method in [16] exploited discrete wavelet transform to generate a key with the help of watermark and binarized low frequency part of the video frame and same is applied on every frame to extract a corresponding key. These keys were used during extraction process. This method fails against filtering attacks since these attacks result in wrong key. Block classification and visual cryptography was used by [17] to embed watermark, where a watermark signal was split into small watermarks based on number of video frames in each shot. Each small watermark was used to generate owner's share which was inserted. This method fails to extract watermark against frame drop attack and also this requires synchronization method to find start position of small watermark.

Therefore, we propose a method to eliminate these disadvantages using multilevel DWT and singular values obtained using SVD. Complete watermark is inserted into single frame rather than distributing into multiple frame to overcome the frame drop attack, hence this method eliminates the usage of synchronization codes to locate starting of the watermark bit. The main contribution of this paper when compared to state of art is computing of four singular value matrices of four sub-bands of DWT instead of one sub band in three level DWT to make it robust against filtering attacks and the way we applied secret sharing to singular values, so that watermark can be retrieved successfully even though two sub bands are filtered out. In secret sharing[18] watermark will be expanded based on host image which makes watermark very secure and also each watermark bit is represented by four bits so that watermark bit can be recovered efficiently even few bits are corrupted at the cost of watermark embedding capacity. We also used chaotic firefly method to select best scaling factor to achieve robustness as well as to preserve the quality of the watermarked video. We discuss the detailed embedding and extraction process in forthcoming sections.

3. Background

This section discusses briefly about the discrete wavelet transform, singular value decomposition and chaotic firefly.

3.1 Discrete wavelet transform

Discrete wavelet transform is being used widely in 1D and 2D signal processing due to its advantages in signal and image processing applications like compression, de-noising, texture analysis and etc. Later on, its usage is carried into watermarking. Discrete wavelet transform (DWT) unlike DFT or DCT [19] represents a given signal with set of basic functions efficiently and flexibly by using filter banks, these basis functions are termed as wavelets. In image processing domain, discrete wavelet transform represents a given image with series of wavelets in multi-resolution manner for effective analysis, also signal can be viewed or analysed both in spatial domain and frequency domain simultaneously. A 2D DWT can be implemented by applying 1D wavelet along the rows and then along the columns to result in 4 sub-bands, each contains specific range of frequency coefficients. These can be used for any kind of applications and as well for watermarking, which uses these sub-bands either for inserting the watermark bits directly or for further processing [20]. Fig. 1 shows one level DWT filter design used for decomposition and Fig. 2 shows the example output of 3-level DWT.

In Fig. 1, LPF represents the low pass filter whereas HPF represents conjugate filter such as

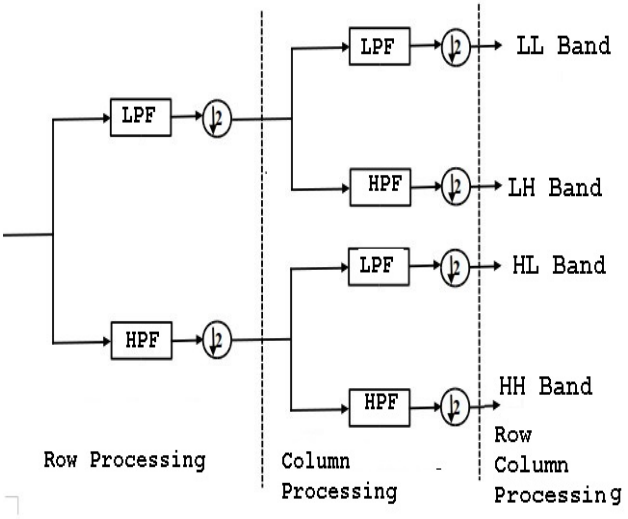

Figure.1 Represents DWT decomposition

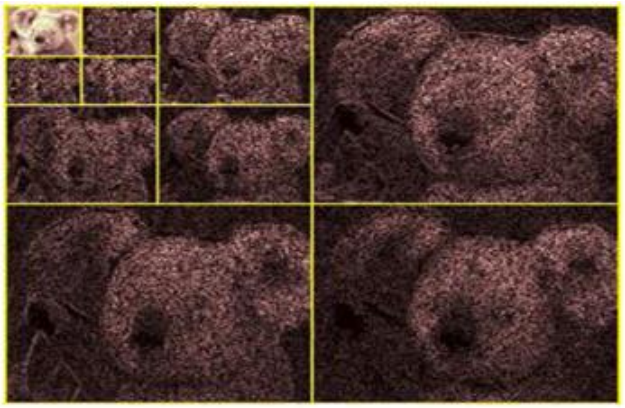

Figure.2 Sample 3-level DWT decomposition

high pass filter and together can be termed as filter banks. In this work, Haar Wavelets are selected due to its simplicity in-terms of operations and it decomposes the signal into four sub band signals. Hungarian mathematician Alfred Haar introduced the Haar wavelets, which is similar to step function. Original signal can be computed by inverse operation of the decomposition filter and is a symmetry of the decomposition filter shown in Fig.1. Instead of down sampling where up-sampling will be used on the given four sub band inputs. All though DWT is old transform domain, still it has been being used in image or video watermarking due to its advantages.

3.2 Singular value decomposition

Singular value decomposition (SVD) is generally used for decomposing the image into sub matrices for removing redundant data in compression applications and also used for watermarking. As name suggests the Decomposition results in three matrices and they are left, right singular vector matrix and diagonal matrix. The diagonal Matrix consists of singular values along its diagonal in decreasing order, where singular value represents the energy of the given signal. These singular values plays an important role in compression and as well as watermarking. One peculiar property of the singular values is small perturbation over signal, these values are not effected much and vice versa. Hence, these are used for watermarking [21].

3.3 Chaotic firefly

Chaotic firefly algorithm [22] is used to find the proper scaling factor to scale the watermark bit during embedding phase such that robustness and perceptual quality will be maintained by doing optimization over given parameters. Chaotic firefly algorithm is an extension of firefly algorithm (FA) in order to improve the efficacy. This enhancement can be done by replacing the random parameters and constants of the FA. Hence, optimal value of the FA can be obtained by using a logistic regression. Logistic mapping is used to replace the parameters and to improve algorithm performance as given Eq. (1)

$$X_i = X_i + I_0 \; e^{\gamma r^2}\left(X_j - X_i\right) + \alpha \, U_i \qquad (1)$$

Firefly algorithm is population based algorithm, in which each member of the population is a candidate solution of the problem that is going to be solved. In Eq. (1), X_i represents the candidate solution; I_o represents light intensity at the source and also can be termed as attractiveness at the source that depends on distance r, fixed light absorption coefficient γ. And α represents a step size scaling factor with respect to U_i randomization parameter. Where in above Eq. (1) first term conveys about position of the i^{th} firefly, second term conveys to social component of moving the firefly i towards the more attractive firefly j with a component α light absorption coefficient of the medium, third term is to represent randomised move of the i^{th} firefly with in the search space. During the evaluation of chaotic firefly algorithm, it tries to calculate value of the objective function for each candidate solution.

This work adopted scrambling method [23] to scramble the watermark for eliminating burst errors, which are resulted from severe attack over watermarked video frame using various signal processing methods. Watermark is inserted into frame after scrambling, when burst errors are occurred during watermark extraction process, these burst errors can be converted to single bit errors using de-scrambling. Hence, these can be corrected easily by using any error correcting codes.

In order to make the watermark more secure, watermark can be shared among multiple samples or each bit of watermark can be represented with multiple bits. This can be achieved by using secret sharing method [24]. The image to be secreted will be represented with n-shares using a pre-determined code book. Few shares are enough to retrieve the original image. This paper have employed a method [24] for generating the share image from the watermark, each bit of watermark and feature vector are extracted from the cover image which has been used to generate share bits of corresponding watermark bit. So, if watermark size is 30x30 then share image size will be four times the watermark size because each bit is represented by four bits. In general, this resultant share is called private share (p-share image) and will be inserted into video as a watermark. During the watermark extraction, same process is employed on watermarked video to extract the public share image called as c-share. This c-share and extracted p-share from watermark extraction process will be used to extract watermark. Dilation or erosion morphological operations can be used to extract exact watermark.

4. Methodology

This section deals with watermark embedding and extraction processes along with corresponding block diagrams.

4.1 Watermark insertion

Methodology involved in embedding a watermark into a video is given in Fig. 3. The input video is fragmented into frames. The blue (B) and red (R) colour channels of each frame are selected for watermarking due to their visibility characteristics. Same watermark approach is used to watermark each R and B channels (components) separately for improving the retrieval accuracy at the cost of computation. Therefore watermarking procedure with one component is explained here. To generate share image, colour component is fragmented into blocks of size 32x32 and then 3 level Discrete Wavelet Transform is applied on each block, This results in four subbands "LL, LH, HL and HH" per each block, where LL component (approximate component) at the output of one level Discrete Wavelet Transform will be used as input to the next level Discrete Wavelet Transform except for first level DWT where input block of an image will be used as input. So, 3-level Discrete Wavelet Transform results in a 4x4 size of four sub bands, let's say LL, LH, HL, HH sub bands. Singular Value Decomposition is applied on four sub bands individually and resulting a three sub matrices for each sub band. Out of three, one is diagonal matrix with singular values along the diagonal direction in decreasing order and other two are said to be right singular vector matrices and left singular vector matrices. The singular value matrices of four sub-bands and each bit of watermark are used to generate share image called p-share based on the table in [24]. Following this, row column transformation is applied on share image for scrambling the watermark in order to overcome the problem of consecutive errors, this helps in correcting single bit errors more easily than bunch of consecutive errors by using error correcting codes. Resultant share image size is double (*2kx2k*) than input watermark size*(kxk)* because each input watermark is shared to four bits so that if at all one or two bits are corrupted due to attacks, still the original bit can be recovered based on majority of the four bits during watermark extraction process. This share image is in the form of binary image and this is converted into bipolar form i.e., matrix having positive ones and negative ones during inserting process.

Each bit of p-share will be inserted into one block of the colour component in Discrete Wavelet Transform and Singular Value Decomposition domain during embedding process with proper scaling factor. Each colour component is fragmented into sub blocks of size 8x8 and then one level Discrete Wavelet Transform is applied, resulting four sub bands of LL, LH, HL and HH of size 4x4. In Discrete Wavelet Transform, we used Haar filter bank due to its simplicity in computation and efficiency. Out of four sub-bands, Singular Value Decomposition is performed on LL (approximate coefficients) band thus resulting in a three sub matrices such as left singular vector matrix, diagonal matrix has singular values along its diagonal direction in decreasing order, right singular vector matrix. Out of three matrices, singular matrix is selected for watermark inserting purpose because minor change in singular values does not affect the quality of the video as well as even for attacks on video may not affect the singular values. Each bit of p-share is added to first singular value of the diagonal matrix based on the Eq.(2) with preselected scaling factor, which is used to compromise the robustness as well as perceived quality of the video. This process is continued on each block till all the bits of p-share are embedded. The Input video resolution is selected such that all bits of p-share are accommodated into a single frame. This opportunity brings the strength to our method in case of frame drop attack when compared to state-of-art method. Frame drop attack is an attack performed by dropping few video frames in between the video to make the watermark extraction system to fail in extracting the watermark. The dropped frames may be consecutive or random frames throughout the video. Where p-share is converted into bipolar form before embedding.

$$S_1 = S_1 + \alpha(sharebit) \quad (2)$$

Where S_1 is first singular value of the singular value matrix obtained from SVD decomposition and α is the scaling factor, which will be obtained using chaotic firefly algorithm and sharebit is the watermark bit obtained from watermark and input video frame. Once the watermark bits are embedded into a colour components, reverse operation of Singular value decomposition that is multiplication of the modified singular value matrix(*S*) with left singular vector matrix(*U*) and right singular vector matrix(*V*) in order *(U*S*V'*) and then inverse Discrete Wavelet Transform will be performed along with modified LL sub band and remaining sub

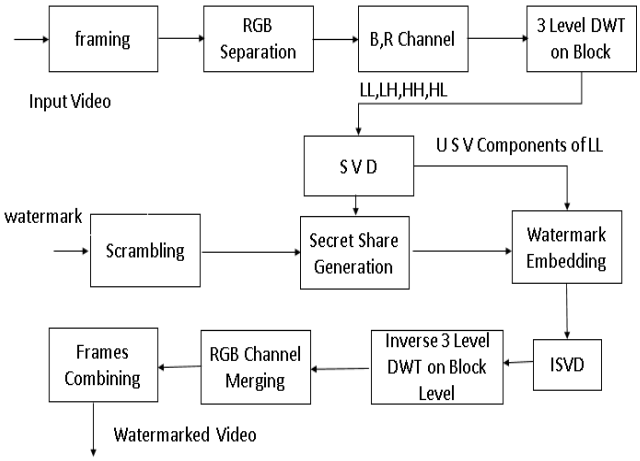

Figure.3 Watermark inserting process into a video

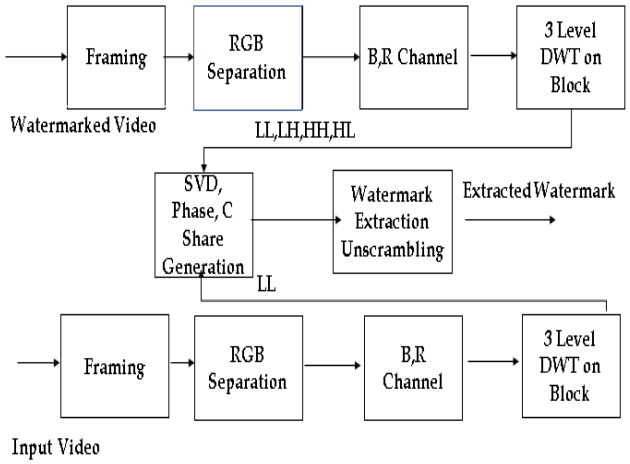

Figure.4 Watermark extraction process from a video

bands such as LH , HL and HH to get back the original watermarked component and then these three components R, B, and G components are combined to form a watermarked frame. The same procedure is applied on B colour component of the video frame and four subbands of each block to make it robust against filtering attacks. Finally, all these frames are combined on the fly using FFMPEG [25] to get back the watermarked video.

4.2 Watermark extraction

The block diagram for watermark extraction is shown in Fig. 4. Watermark is extracted by using both original video and watermarked video. Where R and B components are selected because these components are used for embedding the watermark. From watermarked R component, c-share image is generated by using same procedure applied during p-share generation and the same from B component as well. Embedded watermark is extracted by applying one level Discrete Wavelet Transform, and Singular Value Decomposition on LL component on both R components of input video as well as watermarked video and first singular values of both frames are compared based on majority either one or zero is extracted. The extracted watermark is same size as c-share image. Finally extracted watermark and c-share are used to extract original watermark by performing exclusive-or operation and by using majority voting from block of four bits. Still if any error persists then those can be eliminated by using error correcting codes and by using morphological operations.

4.3 Chaotic firefly algorithm

Chaotic firefly optimisation method should be populated first like other optimisation methods. For this, 15 attacks on watermarked video are performed. The attacks are salt and pepper noise with various densities (0.02,0.2), rotation(-3degrees to 3 degrees), scaling(50% to 150%), cropping ,Gaussian smoothing with various window sizes(3,5,7), histogram equalisation, sharpening, jpeg compression, video compression(mpeg, x264) at various bit rates. Watermark is extracted from each attacked video and both average PSNR on watermarked videos and average number of bits in error are calculated from each attacked video. Eventually, each firefly value is calculated by using objective function as given in Eq. (3).

$$Obj = PSRN + \emptyset \sum_{i=0}^{i=15} ANBE(WM, WM_i) \quad (3)$$

Where *ANBE* is average bits in error on given video, which is the average of number of bit errors over the video frames. *WM* is the original secret shared watermark, WM_i is the extracted watermark from i^{th} attacked video, when $i=0$ means no attack is performed. Φ is the weight factor which will be learned by optimisation and *PSNR* is defined as the peak signal to noise ratio and is computed as given in Eq. (5).

5. Experimental results

In this section, we demonstrate experimental results of the proposed video watermarking method by implementing it in MATLAB and measure performance against a dataset comprises of 140 videos. We also proved this with simulation results, how chaotic firefly algorithm shows its influence on video watermarking to compromise imperceptibility and robustness along with watermark embedding and extraction approach. We did simulations by setting the watermark size to 15x20 and then secret sharing image size becomes double than that of

watermark, that is 30x40, which represents a unique logo assigned to the customer for tracking from where the video is pirated or owner to prove ownership and this is inserted into the video in avi format of size 640x480 using the proposed method. For generating the secret share image, we followed the table given in [24]. Any format of a video can be converted into avi format required for embedding the watermark and the watermarked video is converted back to original video by the FFMPEG tool. Compromise between robustness and imperceptibility is achieved by optimizing the scaling factor in the interval of 10 and the optimized parameter is computed using chaotic firefly algorithm and fixed to 13. The performance of the proposed method is tested on various kinds of video genre. Perceptual visual quality is measured by computing Peak Signal to Noise Ratio (PSNR) as given in below equation and robustness of the method is validated by calculating the number of bits that are in error and then calculated error rate on various kinds of video genre. We also evaluated the performance and robustness of the method against several attacks like median filtering, compression, salt and pepper noise, rotation, scaling, frame drop, frame swap and combination of these.

$$MSE = \frac{1}{mn} \sum_{i=1}^{m-1} \sum_{j=1}^{n-1} (I(i,j) - K(i,j)) \quad (4)$$

$$PSNR = 20\, log(\frac{MAX_t}{MSE} \quad (5)$$

Where *I, K* are the input image and watermarked image respectively. In this experiment, we measured average PSNR means average of PSNR values of videos frames of the watermarked video. Similarly, we measured average number of bits in error means average of number of bits in error frame all the video frames of the watermarked and attacked video. The initial chaotic firefly parameters are set α is 1.0 and γ is 0.01. The Maximum number of iteration is set at 15 and the firefly populations of CFA are 15. The parameter ϕ in 10. To run chaotic firefly algorithm we selected the scaling factors from 10 to 25 and few attacks which were mention earlier. For this we selected sports video as well as news video.

Sample input logo that we considered in this experiment is shown in following Fig. 5 and Fig. 6 shows the scrambled watermark logo shown in Fig. 5, this scrambling is done avoid burst errors. In our case scrambling is done after secret share image generation.

Figure.5 A watermark

Figure.6 Scrambled output of a watermark

(a) (b)

Figure.7 Share images: (a) generated from video frame1 and (b) generated from video frame 2

This input watermark logo is used to generate shared image along with input video frame, it varies from frame to frame and the same is inserted into the corresponding frame as a watermark. Two sample share images from two input video frames are shown in Fig. 7. We have also shown the experimental results of proposed method. First of all quality of the video is tested by measuring PSNR metric that ranges from 44 to 47 depending on video genre for this method. This PSNR [26] is enough to say that this method is acceptable for video watermarking purpose to prove ownership.

Further the robustness can be increased by increasing scaling factor at the cost of quality in sense increase in scaling factor results in decrease in PSNR while increase in retrieval accuracies and the same is shown in Figs.8 and 9, respectively.

We also simulated various manipulations over video(generally these can be termed as attacks) which generally happen while transferring the video over INTERNET, attacks such as rotation, scaling, compression, frame rate conversion and frame drop attack. Various compression methods like mp4 compression, mpeg compression etc. are also performed to prove the robustness of the system. Few of the attacks are simulated using MATLAB and compression attacks are simulated using FFMPEG [25]. The following Fig.10 shows the extracted watermark when no attack occurs from one frame of the avi video.

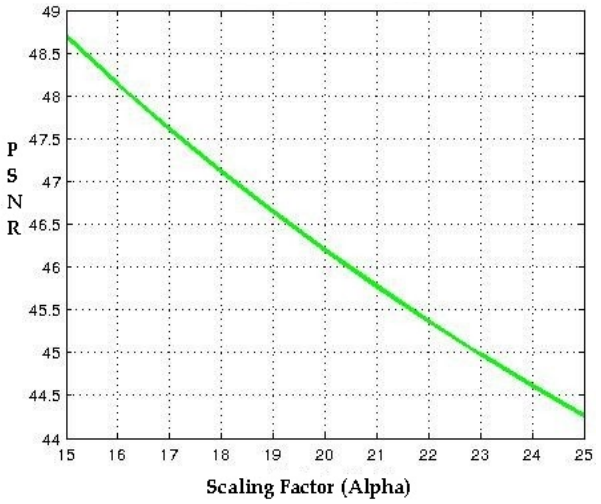

Figure.8 PSNR vs scaling factor

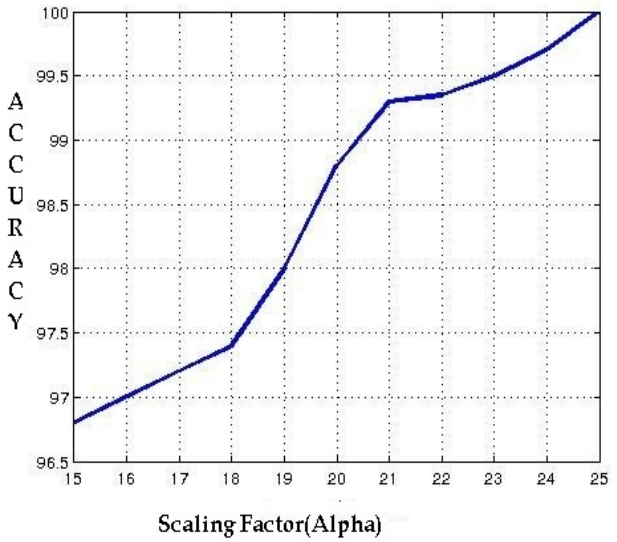

Figure.9 Retrieval accuracy vs scaling factor

Figure.10 Extracted watermark from one frame

Figs. 11 and 12 show when salt and pepper noise is added to the video frames and extracted watermark logo using proposed method when salt and pepper noise with density is 0.02. In this experiment, we achieved the retrieval accuracy of 99.333 percept.

The Table 1 shows the watermark retrieval accuracy in terms of number of bits in error verses various attacks and also compared with the one of the state of art method [27] and [28]. The results state that proposed method is able to show the improvement in number of bits in error. Considered one frame from the video to compare with state of art.

We also evaluated the method by calculating average PSNR to measure imperceptibility and average number of bits in error to measure robustness on various kinds of video genre when rotation attack is -3 degrees. Same is illustrated in Table 2.

Table 3 shows when the attack is mpeg compression at bit rate of 1024kbps. PSNR will be same in every case because it measured when watermark is inserted. Only average bits in error are changed.

Table 4 shows when the attack is x264 compression at bit rate of 2048kbps.

Figure.11 Salt and pepper noise is added with density of 0.02

Figure. 12 retried watermark with accuracy is 99.333

Table 1. Watermark method accuracy

Attack Type	Number of Bits in Error		
	Method [27]	**Method [28]**	**Proposed method**
Rotation 2 degrees	16	9	6
Scaling 200%	6	3	1
Scaling 50%	4	2	1
Cropping 30%	12	5	8
MPEG 2 with 1024 Kbps	9	6	2
Frame Drop (up to 400 consecutive frames)	Not able to sync	0	0

Table 2. PSNR and average bit errors on various video gerne when rotation is -3

Video Types	PSNR(db)	Avg. Bit Error
Sports Videos (foot boll)	46.23	9.23
General Movie	46.13	3.45
Cartoon Video	45.23	2.56
News Video	44.9	5.21
Natural Video (Geographic Channel)	46.89	6.03

Table 3. PSNR and average bit errors on various video gerne when mpeg compression at 1024 kbps

Video Types	PSNR(db)	Avg. Bit Error
Sports Videos(foot boll)	46.23	10.24
General Movie	46.13	11.32
Cartoon Video	45.23	15.23
News Video	44.9	9.23
Natural Video (Geographic Channel)	46.89	8.56

Table 4. PSNR and average bit errors on various Video gerne when mpeg compression at 1024 kbps

Video Types	PSNR(db)	Avg. Bit Error
Sports Videos (foot b0ll)	46.23	12.23
General Movie	46.13	11.69
Cartoon Video	45.23	17.04
News Video	44.9	10.23
Natural Video (Geographic Channel)	46.89	9.23

We also observed that 40% reduction in errors because of secret sharing method.

6. Conclusion and discussion

In this paper, we proposed a solution for video watermarking for claiming ownership especially to counter or prevent illegal online video sharing. This method uses discrete wavelet transform which in turn used singular value decomposition to get singular values because of its robustness even though small change in coefficient does not change its signal characteristics, scrambling method is adopted to remove burst errors and secret sharing is chosen in order to correct the errors by sharing each watermark bit to four bits and retrieved original bit based on majority voting during retrieval process. Selected four subbands to generate secret shared watermark to make the method robust against high pass and low pass filtering methods. Compromise between robustness and quality is achieved by using the chaotic firefly optimisation method for this embedding and extraction scheme. As whole watermark is inserted into single frame, this method is robust against frame drop attack. Experimental section proved the robustness against various attacks while maintaining the watermarked video quality. We simulated various attacks on videos by using FFMPEG and MATLAB. Also the experimental results proved the superior in terms of performance of the proposed method when compared with state of art methods on mentioned attacks. In future work, we would like to improve the retrieval accuracy, try to improve the PSNR and also try to reduce embedding and extraction cost. Adding to the above mentioned point we would like to adopt various optimisation methods and want to compare among them.

References

[1] A. Averbuch, D. Lazar, and M. Israeli, "Image compression using wavelet transform and multiresolution decomposition", *International Journal of IEEE Transactions on Image Processing,* Vol. 5, No. 1, pp. 4-15, Jan 1996.

[2] B. C. Mohan and S. S. Kumar, "A robust image watermarking scheme using singular value decomposition", *International Journal of Multimedia*, Vol. 3, No. 1, pp. 715, 2008.

[3] R.A. Sadek, "SVD Based Image Processing Applications: State of the Art, Contributions and Research Challenges", *International Journal of Advanced Computer Science and Application*, Vol. 3, pp.26-34, 2012.

[4] H. Liu, N. Chen, J. Huang, X. Huang, and Y. Q. Shi, "A robust DWT-based video watermarking algorithm", In: *Proc. of IEEE International Symposium on Phoenix-Scottsdale*, AZ, pp. 631-634, 2002.

[5] S. A. Rathore, S. A. M. Gilani, A. Mumtaz, T. Jameel, and A. Sayyed, "Enhancing Invisibility and Robustness of DWT based Video Watermarking scheme for Copyright Protection", In: *Proc. of International Conf. on Information and Emerging Technologies*, Karachi, pp. 1-5, 2007.

[6] H. Tian and W. Ji, "A Digital Video Watermarking Scheme Based on 1D-DWT", In: *Proc. of International Conf. On Biomedical Engineering and Computer Science*, Wuhan, pp. 1-3, 2010.

[7] C. Wang, C. Zhang, and P. Hao, "A blind video watermark detection method based on 3D-DWT transform", In: *Proc. of IEEE International Conf. On Image Processing*, pp. 3693-3696, 2010.

[8] C. W. H. Fung and W. Godoy, "A novel DWT-SVD video watermarking scheme using side view", In: *Proc. of 5th International Conf. On Signal Processing and Communication Systems*, pp. 1-4, 2011.

[9] A. El Allali, J. Elabbadi, and E.I. Elahaj, "Video object watermarking using 3D-Walsh Hadamard transform and Arnold transform", In: *Proc. of International Conf. On Multimedia Computing and Systems*, Tangier, Morocco, pp. 119-124, 2012.

[10] N. Dey, P. Das, and A. B. Roy, "DWT-DCT-SVD based intravascular ultrasound video watermarking", In: *Proc. of International Conf. on Information and Communication Technologies*, Trivandrum, India, pp. 224-229, 2012.

[11] P. Prathik, R. Krishna, R. A. Nafde, and K. Shreedarshan, "An Adaptive blind video watermarking technique based on SD-BPSO and DWT-SVD", In: *Proc. of International Conf. On Computer Communication and Informatics, Coimbatore*, India, pp. 1-15, 2013.

[12] R. Maharjan, A. Alsadoon, P. W. C. Prasad, A. M. S. Rahma, A. Elchouemi, and S. A. Senanayake, "A Proposed Robust Video Watermarking Algorithm: Enhanced Extraction from Geometric Attacks", *IEEE International Conf. on Multimedia and Image Processing*, Bandar Seri Begawan, Brunei, pp.45-50, 2016.

[13] Li and A. Sui, "A Digital Video Watermarking Algorithm Based on DCT Domain", *IEEE International Joint Conf. on Computational Sciences and Optimization*, Harbin, China, pp. 557-560, 2012.

[14] W. Trabelsi and M. H. Selmi, "Multi-signature robust video watermarking", *IEEE International Conf. On Advanced Technologies for Signal and Image Processing (ATSIP)*, Sousse, Tunisia, pp. 158-163, 2014.

[15] M. Sundararajan and G. Yamuna, "DWT based scheme for video watermarking", *IEEE International Conf. on Communication and Signal Processing*, Melmaruvathur, India, pp. 460-464, 2013.

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

[17] F. Akhlaghian and Z. Bahrami, "A new robust video watermarking algorithm against cropping and rotating attacks", *International Iranian Society of Cryptology Conf. on Information Security and Cryptology*, Rasht, Iran, pp. 122-127, 2015.

[18] S.L. Hsieh, J.J. Jian, I.J. Tsai, and B.Y. Huang, "A color image watermarking scheme based on secret sharing and wavelet transform", In: *Proc. of IEEE International Conf. on Systems Man and Cybernetics*, Montreal, Que., Canada, pp. 213-214, 2007.

[19] M. Ali, "An introduction to wavelets and haar transform", *http://www.cs.ucf.edu/mali/haar*.

[20] K.H. Talukder and K. Harada, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image", *IAENG International Journal of Applied Mathematics*, Vol.36, pp.1-8, 2007.

[21] W. Kong, B. Yang, D. Wu, and X. Niu, "SVD Based Blind Video Watermarking Algorithm", In: *Proc. of First International Conf. on Innovative Computing, Information and Control*, Beijing, China, pp.265-268, 2006.

[22] L. Dos Santos Coelho, D. L. de Andrade Bernert, and V. C. Mariani, "A chaotic firefly algorithm applied to reliability-redundancy optimization", *IEEE Congress of Evolutionary Computation (CEC)*, New Orleans, LA, pp. 517-521, 2011.

[23] R. Rhine and N.T. Bhuvan, "Image Scrambling Methods for Image Hiding: A Survey", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5, pp. 751 – 755, 2014.

[24] S.L. Hsieh, J.J. Jian, I.J. Tsai, and B.Y. Huang, "A color image watermarking scheme based on secret sharing and wavelet transform", In: *Proc. of IEEE International Conf. On Systems, Man and Cybernetics*, Montreal, Que, Canada, pp. 2143-2148, 2007.

[25] *https://ffmpeg.org/*.

[26] Q.Huynh-Thu and M.Ghanbari, "Scope of validity of PSNR in image/video quality assessment", *Electronics Letters*. Vol. 44, No. 13, pp.800-801, 2008.

[27] J. Li, P. Zhong, Y. Zhu, and C. Guo, "Robust wavelet-based watermarking scheme for video copyright protection", In: *Proc. of International Congress on Image and Signal Processing (CISP)* , Dalian, China, pp.125-129, 2014.

[28] S.B. Latha, D.V. Reddy, and A. Damodaram, "Digital Video Watermarking using DWT and Singular Values", In: *Proc. of International Conf. On Information and Communication Technology for Competitive Strategies (ICTCS)*, Udaipur, India, 2016.