A NEW ROBUST AND SECURE APPROACH TO SVD 3 LEVEL DWT VIDEO WATERMARKING FOR FRAME DROPPING AND SOME OTHER ATTACKS

[1]Pawandeep kaur, [2]Sonika Jindal
[1]M.Tech Student, SBS State Technical Campus/PTU,India
[2]Assistant professor,SBS State Technical Campus/PTU,India
[1]pawandeep234@gmail.com, [2]sonikamanoj@gmail.com

***Abstract*— Digital watermarking is used to protect digital content such as images, audio and videos that have been tampered maliciously. Digital media has disadvantage of being prone to easy illegal copying methods such as tampering, piracy, fraud and counterfeiting. Digital video watermarking is a new and merging area of research to exploit different ways in order to prohibit illegal replication and exploitation of digital contents. In this paper, to maintain the quality of video and to ensure the ownership we propose a new SVD-3 Level DWT watermarking embedding technique. Singular value decomposition (SVD) is an important transform technique in robust digital watermarking .We apply the 3 level DWT and SVD on selected frames and embed the watermark into randomly selected frames with the help of secret key to authenticate the video by considering the video quality, robustness and video imperceptibility.**

Keywords—*Digital video watermarking, secret key, scaling factor, 3 Level DWT SVD algorithm.*

I. Introduction

In the past several years a rapid growth in multimedia (audios, videos, images) and illegal transfer of this multimedia content over the internet are becoming important issues in digital era. This leads the development of new technologies providing security to this multimedia content. Digital watermarking is used to protect this sensitive information using different watermarking technologies. Video watermarking is relatively a new technique in multimedia technology. [1] Video watermarking is the process in which watermark is embedded in a video sequence by using a secret key. The amount of information that can be embedded in the video sequence is called payload. The extraction is performed at the other end using the same secret key as shown in Fig: 1**.** The embedded watermark should be robust against variety of attacks such as Subtractive attacks, Distortive attacks, Additive attacks, Filtering, Cropping, Compression, Rotation and Scaling attacks, , so that video can be protected from illegal copying

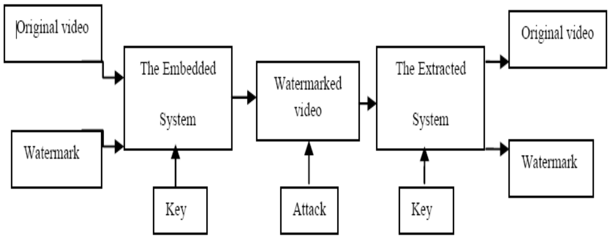

Figure 1. A General Video Watermarking Process

and provide security against several other attacks that only performed on videos such as frame dropping, frame swapping and frame averaging [2].The two types of watermark can be used such as visible watermark and invisible watermark. We can add the watermarks either in the whole frames of video or in certain frames depending upon the requirement [3].

[4] Video watermarking is very different from image watermarking, even though some techniques can be viewed as an extension to it. [1] [4] video watermarking is mainly used in two domains: spatial domain, frequency domain. The first category is spatial domain watermarking in which watermark is embedded in frames by directly modifying the pixel values of that frame[4]. In second category [4] Frequency domain watermarking techniques, first coefficients of transformed video frames are modified and then transformations are applied and at last the inverse process is applied to get the watermarked video. Discrete Fourier transforms (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) [5, 6, and 7] and the Singular Value Decomposition (SVD) [8, 9] is common transforms for watermarking. Watermarking is mostly used in frequency domain because of human visual system is more sensitive to low frequency coefficients and less sensitive to high frequency coefficients. [10] Depending upon the various applications, video watermarking is used in fingerprinting, copyright protection, video authentication, copy control and broadcast monitoring .Apart from these applications video watermarking systems has some properties including effectiveness, data payload, blind or informed detection, false positive rate, capacity, robustness, perceptual transparency, security, cost, sensitivity, and scalability [2].

The rest of the paper is organized as section 2 describes Related work. Section 3 describes Proposed Architecture. Section 4 describes Proposed Algorithm. Section 5 defines Experimental Results. Section 6 demonstrates conclusion.

II. Related work

A. *DWT*

[11] [14] it divides an image into two sections such as in lower resolutions as well as in higher resolutions. Lower resolution means LL components and higher resolution means horizontal (HL), vertical (LH) and diagonal (HH) detail components. The low frequency part is further divided into two sections of high and low frequencies. This process is repeated number of times to compute multiple scale wavelet decomposition. [12] Proposed a method in which 3D DWT is applied using perceptual mask and embedding is performed by weighing the mark through the defined mask and then the Inverse 3D DWT (IDWT) is performed.

- Advantages: More accurate model because its properties similar to HVS and more robust to noise addition.
- Disadvantages: Higher frequencies change the quality of image.

B. *SVD*

It is a mathematical tool which decomposes a matrix into two orthogonal matrices and one diagonal matrix consisting of the singular values of the matrix [13]. The SVD mathematical technique provides an elegant way for extracting algebraic features from an image and improves watermark robustness and resistance against many kinds of attacks [14] [15]. SVD is a useful method to separate the system into a set of linearly independent components. A digital Image X of size MxN can be represented by its SVD as follows:

$$X = USV^T \qquad (1)$$

$$U = [U_{1,} U_{22}, \dots \dots \dots \dots \dots \dots .. U_m]$$

$$V = [V_{1,} V_{22}, \dots \dots \dots \dots \dots \dots \dots . V_n]$$

$$S = \begin{bmatrix} \sigma_1 & & \\ & 0 & \\ & & \sigma_2 \end{bmatrix} \qquad (2)$$

SVD is more applicable in watermarking because of following reasons:

- SVD is able to efficiently represent the intrinsic algebraic properties of an image, where singular values correspond to the brightness of the image.
- Singular values have good stability, which means a small perturbation

added to an image will not significantly change the corresponding singular values.[18]

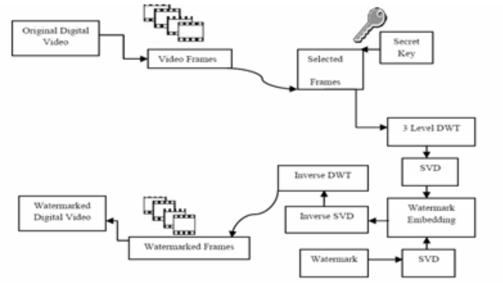

Figure 2. Procedure of watermark embedding

III. Proposed architecture

The proposed method effectively hides the secret data into video using existing video watermarking techniques. Fig: 2 give a complete overview of data flow in proposed algorithm. This method uses some frames of video to hide the secret data. The frames selected to hide secret data are random frames and not sequential frames. Hence each frame that contains the secret data can be identified using secret key, a 10 digit number provided by user. The selection of frames is done by using several functions that are made up from secret key. So, watermark is embedded in whole video and not in some parts of video. We also set up a passkey identifier to give only four trials to the user and if the user inserts more than 4 wrong keys then it means he/she is trying to find out the watermarked frames by trying random keys. If four wrong entries are made by user then the video will be damaged leaving no data behind.

IV. Proposed algorithm

In this section, we have discussed some motivating factors in the design of our approach to video watermarking. We have used DWT and SVD for developing the algorithm. Among various tools, SVD and DWT are more reliable in digital watermarking. Due to the fact of localization in both spatial and frequency domain, wavelet transform is the most preferable transform among all other transforms. After converting the video into frames, we have applied 3 levels DWT on selected frames. In the next stage, the SVD is applied to selected sub-bands and embed the same original watermark by modifying the singular values. Embedded watermark in middle frequencies increases the robustness to variety of attacks. The procedure of embedding a digital watermark into the original video is depicted in Fig: 2. After that, inverse SVD and inverse DWT is applied in order to reconstruct the watermarked digital video. After getting the watermarked video the extraction process is performed at other end in order to check the extracted watermark resembles with original one or not.

A. *Watermark embedding algorithm*

- Apply DWT to the selected frames repeatedly up to the third level.

- Perform SVD transform on approximation and all the detail parts in third level of wavelet transform, f $_Q= U_QS_QV^T$ Where $Q \in \{LL3, LH3, HL3, HH3\}$.

$$f_Q=U_QS_QV^T \quad (1)$$

- Perform SVD transform on watermark,

$$W = U_WS_WV^T{}_W \quad (2)$$

- In general, embedded watermark at this stage. Modify the singular values of approximation and all the detail parts with the singular values of the watermark as:

$$\gamma_Q^* = \gamma_Q + \alpha_Q\gamma_W \quad (3)$$

- Here, is scale factor of combined transform, which value is 0.04.
- Take inverse combined transform and reconstruct the watermarked video.

B. *Watermark extraction algorithm*

- Apply DWT to selected watermarked frames repeatedly up to the third level.
- Apply SVD transformation on approximation and all details parts up to the third level of wavelet transform, Where $Q \in \{LL3, LH3, HL3, \text{and } HH3\}$ and get the combined transform coefficient γ_Q^*

- Extract singular values of watermark from approximation and all detail parts.

$$\gamma_{W^*}^{Q} = \frac{\gamma_Q^* - \gamma_Q}{\alpha_Q} \quad (4)$$

- Extract the watermark from video frames.

$$W_Q^* = U_W S_Q^* V_W^T \quad (5)$$

- After detecting all estimates of watermark, sum up all these estimates and normalized $\overline{W_Q^*}$ between [0, 1].
- Reproduced the watermark,

$$W_Q^* = \sum_{i=1}^{Q} w_Q^* \quad (6)$$

V. Experimental results

The experimental results are as below which show original frames and corresponding watermarked frames. We test the proposed watermarking algorithm with different variations using colored host video clips. Each video clip is partitioned into different number of frames. We employed “Rhinos” video sequence in AVI format where total number of frames we calculated is 114 and selected 10 random frames to embed watermark such as “logo1.png” of size (128 × 128) in that frames as shown in Fig: 4. The 10 random original frames are shown in Fig: 3 and their corresponding watermarked frames are shown in Fig: 5. Watermarked Video quality was estimated by SSIM, PSNR, BER and MSE.

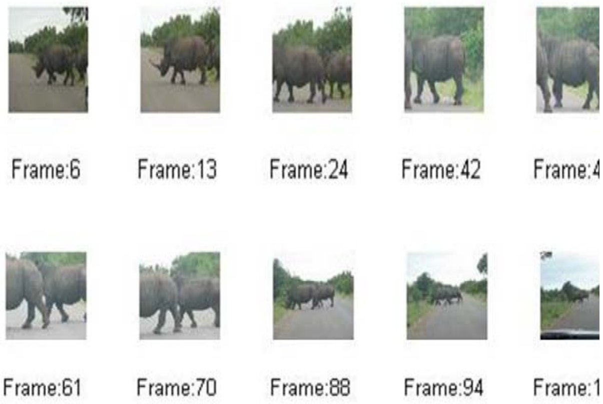

Figure 3. Original Frames

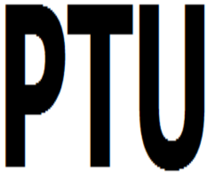

Figure 4. Watermark Image

Figure 5. Watermarked Frames

TABLE I. CALCULATED VALUES OF SSIM,PSNR,BER AND MSE OF WATERMARKED VIDEO

Video	Frame no.	SSIM	PSNR	BER	MSE
Rhinos	6	0.99	52.70	0.01	0.12
	13	0.99	53.20	0.01	0.12
	24	0.99	53.31	0.01	0.12
	42	0.99	52.77	0.01	0.12
	46	0.99	52.35	0.01	0.12
	61	0.99	52.63	0.01	0.12
	70	0.99	52.97	0.01	0.12
	88	0.99	53.92	0.01	0.12
	94	0.99	53.44	0.01	0.12
	106	0.99	53.16	0.01	0.12

We then tested the robustness and quality of watermarked video using a scaling factor 0.04 and different performance evaluation metrics. For each frame we have calculated the SSIM, PSNR, MSE and BER as shown in above Table I.

A. *To check the imperceptibility of watermarked video*

The PSNR is a quality metric used to determine the degradation in the embedded image with respect to the host image or also defined as ratio between maximum power of a signal and power of distorted signal [16]. It is most easily defined via the mean squared error (MSE) as:

$$PSNR = 10log_{10}\frac{L*L}{MSE}$$

The MSE [16] defined it as average squared difference between a reference image and a distorted image. It is calculated as:

$$MSE = \frac{1}{XY}\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j)-e(i,j))^2$$

The BER [16] defined it as the ratio that describes how many bits received in error over the number of the total bits received. It is often expressed as percentage and calculated by comparing bit values of embedded image and cover image.

$$BER = P/(H*W)$$

The SSIM is a method for measuring the similarity between two images. SSIM is designed to improve on traditional methods like peak signal to noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception. It is calculated by formula given below:

$$\mathrm{SSIM(x,y)}=\frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)}$$

The value calculated shows that propose DWT-SVD based video watermarking algorithm is imperceptible. The calculated PSNR value is 53.05db which shows quality of watermarked video appear visually identical to the original one and there is no degradation in visual quality. The value calculated for SSIM is 0.99 which shows the structural similarity between original video and watermarked video.

In order to check the quality of extracted watermark, the normalized Cross-correlation (NC) value between the original watermark and extracted watermark is calculated for different frames using scaling factor 0.04, which is defined as:

$$NC=\frac{\sum_{i=0}^{M_1}\sum_{j=0}^{M_2}[W(i,j)W'(i,j)]}{\sum_{i=0}^{M_1}\sum_{j=0}^{M_2}[W(i,j)]^2}$$

Where W and W` represent the original image and extracted watermark image, respectively. The watermark extraction using scaling factor 0.04 is shown in Fig: 6 which show that correlation value of extracted watermark is near to 1 and extracted watermark is same as original one. The values of PSNR, MSE, SSIM and BER for 10 random frames are calculated as shown in Fig: 6, Fig: 7, Fig: 8 and Fig: 9.Also the correlation coefficient of extracted watermark is shown in Fig: 10.

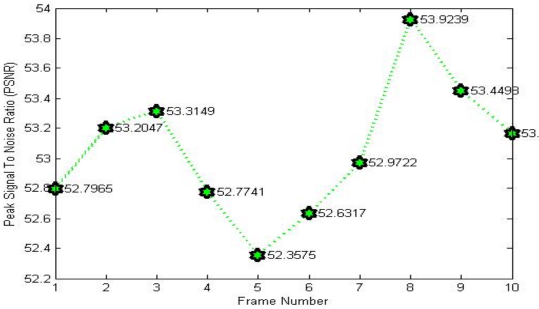

Figure 6. PSNR values of watermarked video for 10 frames

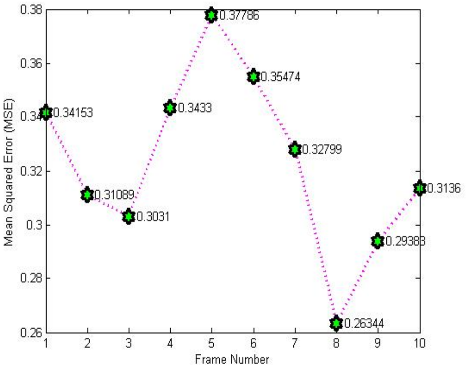

Figure 7. MSE values of watermarked video for 10 frames

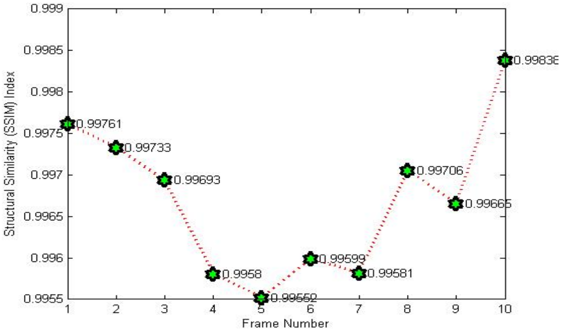

Figure 8. SSIM values of watermarked video for 10 frames

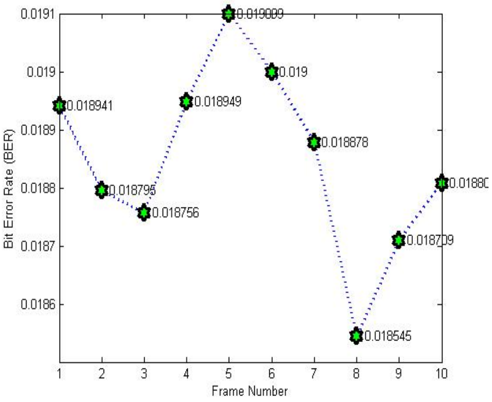

Figure 9. BER values of watermarked video for 10 frames

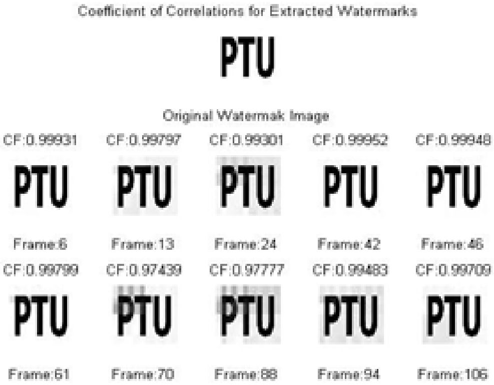

Figure 10. Corelation coefficient of extracted watermark with scaling factor 0.04

B. *Choice of scaling factor*

It is actually a hard step for choosing the suitable scaling factor. Usually, the scaling factor is chosen to be a scalar value. In most of literature the scaling factor is chosen between 0 and 1[17].Table II shows the SSIM, PSNR, MSE ,BER of the watermarked video and the correlation coefficient (NC) of the extracted watermark for several scaling factors. From this table, the higher scaling factor is, the worse the robustness and invisibility of watermark will be.

TABLE II. AVERAGE VALUES OF SSIM,PSNR,BER AND MSE FOR WATERMARKED VIDEO AND EXTRACTED WATERMARK USING VARIOUS SCALING FACTORS

Different parameters of watermarked video and Normalized Cross-Correlation values for extracted watermark						
Video	**Scale factor.**	**SSIM**	**PSNR**	**BER**	**MSE**	**NC**
Rhinos	0.9	0.9151	38.557	0.02	9.08	0.92
	0.5	0.9539	40.509	0.02	5.80	0.95
	0.1	0.9960	50.122	0.19	0.63	0.98
	0.04	0.9992	53.05	0.01	0.12	0.99

C. *To check the robustness of extracted watermark*

To check the quality of extracted watermark we applied several attacks on 10 random frames in which the watermark is inserted. The attacks applied are Gaussian attacks, speckle attacks, salt& pepper attacks, scaling attacks, blur, Gaussian filtering and circular filtering. The calculated PSNR, BER and normalization correlation coefficient (NC) for different attacks are shown in Table III.

TABLE III. CORELATION COEFFICIENT VALUE UNDER VARIOUS ATTACKS

Attacks	**Correlation Coefficient**
Gaussian Noise (mean=0, var=0.001)	0.97
Speckle Noise (mean= 0,var=0.001)	0.97
Salt & pepper (d=0.01)	1
Scaling [256 256]	0.95
Blur	1
Circular filtering(radius=5)	1
Gaussian filtering [5 5], σ =0.1	1

VI. Conclusion

The proposed algorithm is more secure than the conventional algorithms due to the use of an encryption key for the selection of the random frames to be watermarked. And at time of extraction process same encryption key is needed and if key is wrong then nobody can find the watermarked frames. The values of correlation factor between the extracted watermark and original watermark after these various attacks is closer to 1 or almost one which shows that proposed method is robust to various attacks. The calculated values of parameters show the high imperceptibility of the algorithm. Also the algorithm is simple blind algorithm, more secure and highly robust against frame dropping because of random frames & other manipulations.

Acknowledgment

This is to express my sincere gratitude to Dr. Satvir Singh, Associate Professor, Department of Electronic & Communication Engineering, SBS State Technical Campus, Ferozepur (Punjab), India, for sparking in me the enthusiasm and initiative to discover and learn. I am truly thankful to him for guiding me through the entire paper and being as a motivator in this learning curve.

References

[1] Jayamalar, T and Radha, V, “Survey on digital video watermarking techniques and attacks on watermarks,” International Journal of Engineering Science and Technology, vol. 2, Pp. 6963-6967, 2010.

[2] Potdar, Vidyasagar M and Han, Song and Chang, Elizabeth, “A survey of digital image watermarking techniques,” Industrial Informatics, 2005.

[3] Madia, Jigar and Dave, Kapil and Sampat, Vivek and Toprani, Parag, “Video Watermarking using Dynamic Frame Selection”.

[4] Doerr, Gwena and Dugelay, Jean-Luc, “A guide tour of video watermarking,” Signal processing: Image communication, Elsevier, vol. 18, Pp.263-282,2003.

[5] Tay P, Havlicek JP. “Image watermarking using wavelets”, Pp. 258–261, 2002.

[6] Kundur D, Hatzinakos D., “Digital watermarking using multi-resolution wavelet decomposition”.Int Conf Acoust Speech Signal Proc, Pp. 2969–72, 1998.

[7] Wu C, Zhu W-P Swamy MNS. , “A watermark embedding scheme in wavelet transform domain”. In: IEEE Region 10 Conference Proceedings: Analog and Digital Techniques in Electrical Engineering, vol. A, Pp.279–82, 2004.

[8] Loukhaoukha K, “ Chouinard J-Y, “Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification.” In: IEEE. Pp .177–82, 2009.

[9] Gorodetski V, Popyack L, Samoilov V, Skormin V. “SVD based approach to transparent embedding data into digital images,” In: Proc. International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS’01). 2001

[10] Lu, Gaoyan and Zhang, Yongping and Liang, Fengmei and Zheng, Dechun,“Survey of Video Watermarking” *Video Engineering*,vol.21, Pp .009,2012

[11] Sinha, Sanjana and Bardhan, Prajnat and Pramanick, Swarnali and Jagatramka, Ankul and Kole, Dipak K and Chakraborty, Aruna,“ Digital video watermarking using discrete wavelet transform and principal component analysis,” *International Journal of Wisdom Based Computing,*vol.1, Pp 7--12, 2011.

[12] Campisi, Patrizio and Neri, Alessandro,“ Video watermarking in the 3D-DWT domain using perceptual masking,” *IEEE*, vol.1, Pp.I--997, 2005.

[13] K.-L. Chung, W.-N. Yang, Y.-H. Huang, S.-T. Wu, Y.-C. Hsu, “On svd-based watermarking algorithm,” *Applied Mathematics and Computation* Pp 54–57, 2007.

[14] Preda, Radu O and Vizireanu, Dragos N,“ A robust digital watermarking scheme for video copyright protection in the wavelet domain,” *Measurement , Elsevier,*vol. 43, Pp 1720—1726,2010.

[15] Rastegar, Saeed and Namazi, Fateme and Yaghmaie, Khashayar and Aliabadian, Amir,“ Hybrid watermarking algorithm based on Singular Value Decomposition and Radon transform,”*AEU-International Journal of Electronics and Communications*, vol. 65, Pp 658—663,2011.

[16] A. K. Singh, N. Sharma, M. Dave, A. Mohan, “A novel technique for digital image watermarking in spatial domain,” *in: Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, IEEE,* pp. 497–501, 2012.

[17] Mohammad, Ahmad A and Alhaj, Ali and Shaltaf, Sameer, “An improved SVD-based watermarking scheme for protecting rightful ownership,” *Signal Processing Elsevier*, vol. 88, Pp 2158—2180,2008.

[18] Rajab, Lama and Al-Khatib, Tahani and Al-Haj, Ali, “Hybrid DWT-SVD video watermarking,” *Innovations in Information Technology, 2008. IIT 2008. International Conference on, IEEE,* , Pp 588--592,2008.