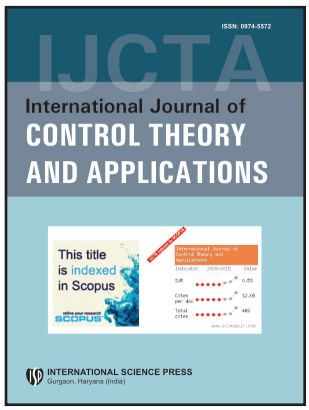


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 43 • 2016

A Novel Compressed Video Watermarking Model using Hash based Encryption and Decryption Algorithm

T. Srinivasa Rao[a] and Rajasekhara Rao Kurra[b]

[a]*DCSE Dept, JNTUK, Kakinada, Assistant Professor, Andhra Loyola Institute of Engineering & Technology, Vijayawada, A.P, India. Email: Srinivas123fast@gmail.com*

[b]*CSE Dept, JNTUK, Kakinada, Professor & Director, UshaRama College of Engineering & Technology, Telaprolu, A.P, India. Email: krr_it@yahoo.co.in*

Abstract:

Background/Objective: Today, with the advancement of internet and technology security of information has become the prime concern. Extensive amount of research has been carried out since years to provide secure and reliable environment for video watermarking. The objective of this research paper is to propose a novel lossless video compression scheme on large video files to speed-up the watermark embedding and extraction process.

Methods/Statistical Analysis: Hashing technique accepts variable-length message as input string and produces fixed-length digest as output after processing. SHA cannot prevent attacks and collisions of hash values.

Findings: Experimental results show that novel chaotic hash model has high computation speed and accuracy compared to traditional compressed video watermarking models.

Applications/Improvements: From the new model, PSNR obtained is higher and the correlation computation of the proposed model is found to be better than the traditional video watermarking models. In future, this work can be extended to web based video watermarking process on the video streaming applications.

Keywords: Video watermarking, DCT, DWT, chaotic hash.

1. INTRODUCTION

In last decade, there is huge development in video encryption and compression technology. It is one of the current field of study that emerge with good algorithms for validation and copyrighting along with good compression techniques and codec's. For the copyright matters, video watermarking is evaluated as one of the finest technique. This paper will cover some of efficient watermarking techniques used in past few years. In it, we will summarize their notions, structural model and their methods for achieving specific standards along with different compression techniques. Fast collaborative social networks and latest cutting edge technological enhancements with an extensive number of players and end users have developed an environment where huge number and volume of digital data is being shared. This data is in the form of pictures, videos or information.

A huge number of streaming servers, video sharing applications and ease of access to these videos have paved the way to unlimited copies of data and have drawn a new issue of data and copy write protection. Similarly, huge efforts have been put in provision of algorithms with better video compression standards and codec's. These algorithms are consequently providing improved video quality and resolution with more data transfer. This transfer of video needs to be equipped with a secure mechanism using an efficient encoding scheme. Video watermarking is a desired technique with compression and encryption methods which is best fit in this case. There are numerous watermarking schemes which have been proposed in last few years which embed owner information and some other features visible or invisible into the video which can be extracted and verified later on. [2]

Watermarking is indeed a solution to the issue of copyright protection specifically for multimedia data in current era of social and next generation networks. More importantly, as there are numerous video sharing applications, video communications over WIFI and internet is resulting in need of digital right protection. So, video encryption along with digital watermarking to videos serves the purpose. Although there are many factors which needs to be considered before selecting the right algorithm for watermarking. These factors are robustness, complexity, noiselessness, volume, bit rate, PSNR and synchronization. [3][4]

Although video is also a sequence of still images or frames but digital video watermarking is bit different than an image watermarking. It needs to fulfill some other requirement than simple image watermarking, such as video coding methods, redundant information between different continuous frames and specific attacks on video. Moreover, every video watermarking methods needs to be optimized structure so that the primary goal is to reduce time complexity in process of implementation of watermarking in the video. So it needs better compression technique also so that the size of video may need less bandwidth to travel over the channel. [7]

Shwu-Huey Yen 2008[1] presented a scene based video watermarking model which is developed considering the decent simplification capacity of Support Vector Machine. This algorithm implants watermarks in randomize location in each frame in one scene with the ability to add only one watermark in long scene with same values. SVM algorithm train itself for the rest of the data and dynamically watermark all other frames. Watermark extracted after processing is basically the average value of all the frames. The results of the algorithm depicted that it is robust to TFA, video compression and WER collusion attacks.

Robert Facciol 2010[2] presented error recovery approach which embeds a reversible watermarking method to keep H.264/AVC video codec based contents. This algorithm uses "reversible watermarking" to be included with error detection mechanism. This watermark is embedded into every Macroblock of video defined by the system. On other end, decoder detects the watermark of Macroblock and detect a corrupted block. This technique also recovers the original video after extraction and detection of watermark. In this way, video quality remains the same as before watermarking. This method gives a PSNR value up to 2.6 dB which is extensive improvement with reference to the standards with minute change in its complexity.

Charles Way Hun Fung 2011[3] proposed a technique which embeds information in side view rather than in frame as per normal approach. By using this technique, it adds the watermark by changing the reference of the video in the frames. It is done using defining the same width and height of frames unlike the original one using dimensions. Then it converts the greyscale image on luminance in YUV transformed video using DWTSVD watermarking. This method has provided robustness for recovering from attacks such as frame attacks, noise addition, or MPEG compression.

Ekta Walia 2012[8] presented a method in which Weber's descriptor is used to authenticate watermarked transformed image as well as the original watermarked image. Two factors are used to verify the actual watermarked image as well as transformed image. These factors are Euclidean distance and normalized correlation coefficient.

Satyendra N.Biswas 2013[5] presented technique in which single watermarked image is segmented into multiple binary images then these are incorporated in a sequence of video. By changing the wavelet coefficients, the watermark based on spatial spread spectrum is directly infused into a bit streams with better compression technique. This approach shows a good response and robustness to handle spatial attacks which includes frame average and scaling and time domain attacks such as shifting and frame dropping.

Prathik P 2013[4] suggested a concept for watermarking videos. This technique uses "Adaptive Frame Selection using SD-BPSO". This method mainly focused that this technique effect bare minimal to the quality of the video. PSNR was used to determine the validity of technique. Multiple attacks are used to check the robustness of algorithm and found it good for cropping, rotation, image shift, image sharpening and histogram equalization. To measure the efficacy of the system for retrieving back video watermark, Bit Error Rate (BER) is used.

Archana Aniyan 2013[6] used a method called as discrete cosine transform (DCT). This method used blind watermarking technique for digital media Beagle Board was used for its hardware implementation. This technique also displayed its robustness for numerous attacks and equally good for compression.

C. D. Rawat 2014[7] used mix method. This research used Discrete Cosine Transform, Singular Value Decomposition and Discrete Wavelet Transform as a combined technique. The sequence of applicability of these techniques were DCT-SVD, DWTSVD and DCT-DWT-SVD. PSNR and Correlation were used to measure the efficiency of the system.

Farhan Alenizi 2015[9] proposed a wavelet watermarking scheme for video authentication. A DWT process is implemented using orthonormal filters, where the Y-components of the frames in video were divided using DWT technique, sub bands were embedded with watermarks. After this, reconstruction of the video is performed. To increase the security of the method, the filters for DWT subbands are random in nature. High efficiency video coding technique is used to measure the performance of the system.

Neena.P.M 2015[11] used a method for digital watermarking in which frequency domain transform methods (DCT, DFT, DWT) were implemented for embedding watermarks. The decoding was developed upon the side information which produced at the time of watermarking. Method compares the PSNR and BER and applied the spatial attacks and compression attacks. This technique depicted that DWT was a better technique of these three techniques.

Rupali D. Patil 2015[10] came up with a technique called effective fragile video watermarking for watermarking and retrieving in DCT with more transparent mechanism. Every frame is embedded with two watermarks. One video watermark contains the bit value for micro block number and frame sequence while second watermark contains number of bits for "digital signature of hash value of the frame in frequency domain". By using highest non-zero coefficient of quantized DCT coefficient, every frame is watermarked one by one. One of the watermarks is used to localize the area identified by the other watermark.

Nitin Arvind Shelke 2016[12] used Genetic Algorithm as optimized and hybrid based robust digital video watermarking scheme. The optimization is performed in the proposed system with the help of genetic algorithm. The quality of this method for watermarking was determined by using NC and PSNR. The PSNR calculated using our approach is off 50.48 db which is far better than existing approaches.

Sneha Kadu 2016[13] technique was based on DWT-based video watermarking which is simple and efficient. Discrete Wavelet Transform was used one every frame of video to attain frequency domain values for a sequence of video. This technique uses low and high pass components where low pass is required to generate key value for the frame. That encrypted key is then used to decrypt the watermark and video sequence. Blind

watermark needs key value for information of invisible watermark. By applying several attacks, its performance is evaluated based on factors such as NC, PSNR, or SSIM.

The major challenge in existing video watermarking models is the synchronization problem, in which the embedded position of the watermark gets changed due to scaling or rotation.

The main limitations identified in the above related models from [1] to [13] are:

1. Low compression ratio.
2. Executes maximum number of processing steps.
3. The ability of the models to work on specific hardware.
4. The ability of the algorithm to operate in traditional hash models.
5. As the size of the video increases, these models fail to process large number of streaming frames.
6. Watermark pixel transformation is not possible.
7. Quality of the video decreases when n number of frames is added.
8. Direct change of a compressed bit stream is generally difficult.

In our research work, a novel video compression based watermarking model for video protection and authentication is implemented.. In this model, we have proposed a novel lossless video compression scheme on large video files to speed-up the watermark embedding and extraction process.

2. PROPOSED METHOD

Hashing technique accepts variable-length message as input string and produces fixed-length digest as output after processing. SHA cannot prevent attacks and collisions of hash values which are the major lacunae of this algorithm. These algorithms are not very efficient for real-time applications which are dynamic in nature. SHA is also categorized into different algorithms- SHA, MD5 etc. To overcome this problem, chaotic-based hashing techniques are developed which are non-linear, random and dynamic in nature. It can be represented by either discrete or continuous systems.

Novel Chaotic Hash Algorithm:

Input: Watermark image data or Compressed Video

Output: Computed Hash Value.

Procedure:

For each block in the Image

Read binary data *f*,

Let N bet the number of partitions, each with bytes bits.

Divide data-file into N partitions each with bytes.

N = *f*.size/1024;

For each frame data

Do

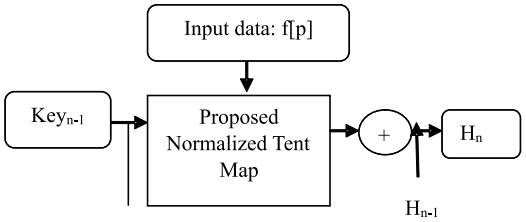
For each block partition p in N

Do

Process data $f[p]$ in the Chaotic Tent computation as

Normalize $f[p]$ to [0,2].

$$Ct(x) = mf(x), \text{ where, } m \in [0, 0.5).$$
$$= m(1 - f(m)), m \in [0.5, 1]$$
$$f(x_{n+1}) = Ct(x_n)$$



Done

Final hash is computed as

$\text{Hash}(H_n) = k_{n-1} \oplus \text{Hash}(H_{n-1})$

Done

Done

Proposed Image Encryption and Decryption algorithm: Encryption algorithm encrypts the message using policy pattern structures. Algorithm uses three patterns with homomorphic encryption and decryption process. Additive and Multiplicative homomorphism takes two inputs and generate secure encrypted values as output.

For each block partition HashData [i] data

Do

For each byte j in HashData[i]

M_{e1} = HashData[i][j]; //central pixel

M_{e2} = HashData[i + 1][j]; //neighbor pixel

Additive Homomorphic Encryption

$\text{Enc}(M_{e1} + M_{e2}) = p \times \text{Enc}(M_{e1}) + q \times \text{Enc}(M_{e2})$;

Where p and q are the max and min values in the neighbor pixels.

$\alpha = p$;

$\beta = q$;

$\gamma = p + q$;

Multiplicative Homomorphic Encryption

$$\text{Enc}(M_{e1} \,.\, M_{e2}) := p.q(\text{Enc}(M_{e1}).\text{Enc}(M_{e2}));$$

$$\text{Enc}(M_1) := \text{Enc}(C_0) = (C_0 + \gamma \times \beta) \text{mod p.n where } n = \alpha \times \beta;$$

$$\text{Enc}(M_2) := \text{Enc}(C'_0) = (C'_0 + \gamma \times \beta) \text{mod q.n where } n = \alpha \times \beta;$$

$$\text{Enc}(M_1 + M_2) := \text{Enc}(C_0 + C'_0) = \text{Enc}(C_0) + \text{Enc}(C'_0);$$

$$:= (C_0 + \gamma \times \beta) \bmod \text{p.n} + (C'_0 + \gamma \times \beta) \bmod \text{q.n} \quad (1)$$

$$\text{Enc}(M_1 \,.\, M_2) := \text{Enc}(C_0 \,.\, C'_0) := \text{Enc}(C_0) \,.\, \text{Enc}(C'_0);$$

$$:= (C_0 + \gamma \times \beta) \bmod \text{p.n.} + (C'_0 + \gamma \times \beta) \bmod \text{q.n} \quad (2)$$

Done

Chaotic Hash Based Watermark Embedding Process on Compressed Video

Step 1: Load the video

Step 2: Apply JMF video compression

Step 3: Convert each compressed video frame from RGB to Y, Cb, Cr format.

Step 4: Compute the steps 5 to 10 for the Y component of each compressed frame.

Step 5: Perform 3-level DWT on Y-component.

Step 6: Compute Hash (Watermark image).

Step 7: Encrypt Computed Hash using the Y-Component as key.

Step 8: Save the encrypted hash value in a file.

Step 9: Perform SVD model on the 3-level DWT and Watermark *w*.

Step 10: Perform Watermark embedding process using the following equation

$$\text{WEmbed WE}(i) = \text{SVD}_i(\text{DWT(3-Level)} + \varphi \,.\, \text{SVD}_i(w)$$

Step 11: Apply inverse SVD and 3-level IDWT to embedded watermark on the frame.

Step 12: Save the embedded watermark video.

In the above algorithm, a source video is taken as input for watermark embedding process as shown in Figure 1. Source video is compressed using the JMF java video codec. Next, convert each compressed video frame from RGB to Y, Cb, Cr format. In the next step, Y component of each compressed video frame is extracted to perform 3-level DWT, Hash value and watermark encryption process. Finally, watermark embedding process is performed with the SVD model.

Chaotic Hash Based Watermark Extraction Process on Compressed Video

Step 1: Load the Watermarked Video

Step 2: Apply JMF video Decompression

Step 3: Convert each compressed video frame from RGB to Y, Cb, Cr format.

Step 4: Compute the steps 5 to 7 for the Y component of each compressed frame.

Step 5: Perform 3-level DWT on Y-component.

Step 6: Perform SVD model on the 3-level Embedded DWT and Watermark *w*.

$$(\text{WEmbed WE}(i) - \text{SVD}_i(\text{DWT(3-Level)}))/\varphi = \text{SVD}_i(w)$$

Step 7: Perform Watermark Extraction process using the following equation

Step 8: Decrypt Computed Hash using the Y-Component as key.

Step 9: Compute Hash (Extracted watermark image).

Step 10: Check the integrity verification.

Step 11: Restore the original video

In the above extraction algorithm, a watermarked video is taken as input for source video extraction as shown in Figure 2.

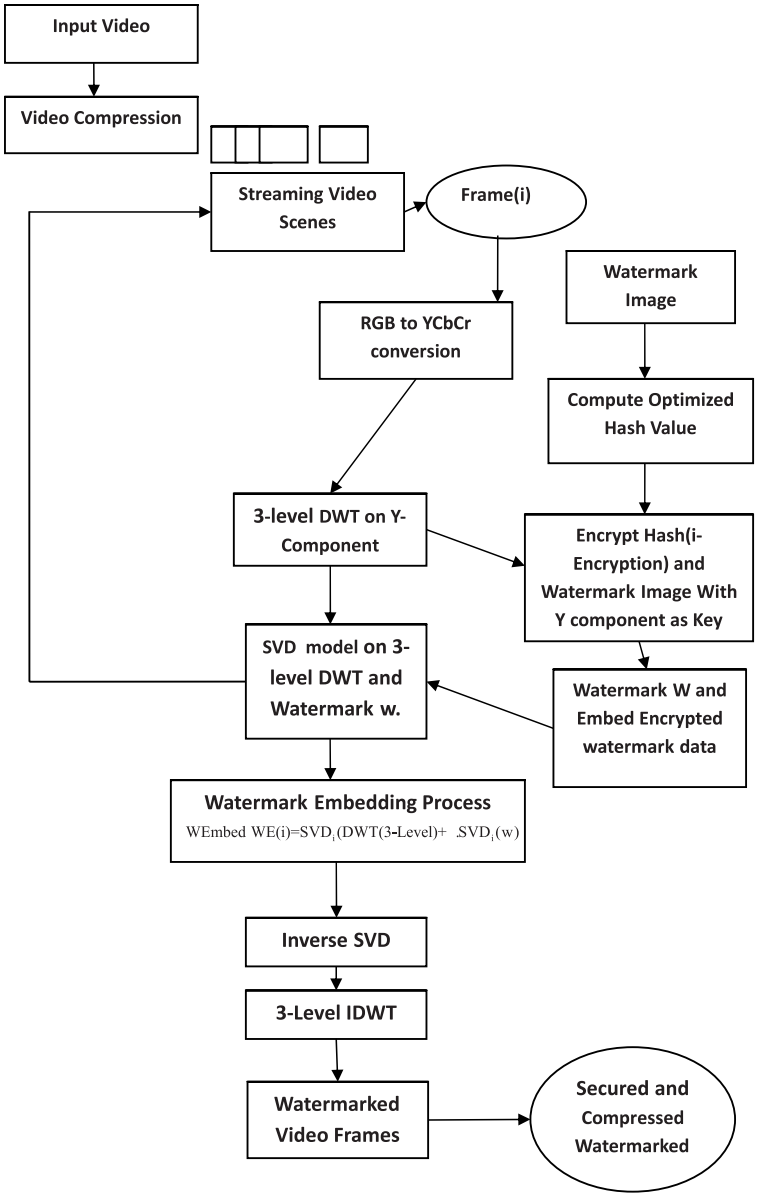


Figure 1: Proposed Embedding Process

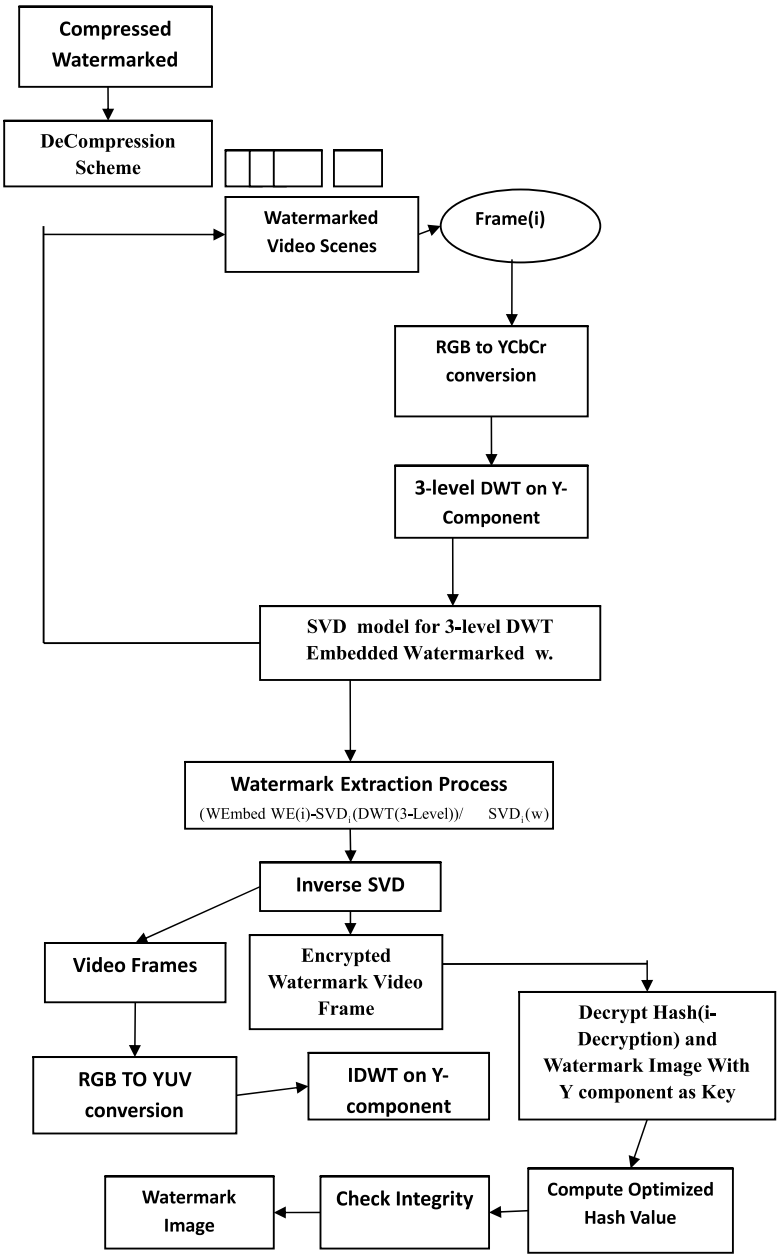


Figure 2: Proposed Extraction Process

3. PERFORMANCE ANALYSIS

To evaluate the performance of proposed watermarking model, standard high resolution video clips of size 1024x1024 are used. In this section, we will evaluate the performance of the proposed model against different types of video sets and attacks. The metrics used in our model are correlation and PSNR between the source video frame and the extracted watermark. Figure 3-6 describe the input video frame, compressed video frame, input watermark logo and embedded watermark frame.

In the experimental evaluation process, if the extracted image is close to the original source image, then MSE is small and PSNR value is large. The MSE and PSNR values are computed using the following equations.

Figure 3: Input source video

Figure 4: Input Compressed Video File

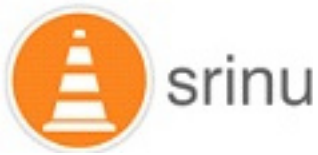


Figure 5:Watermark logo

Figure 6: Embedded Video Watermark

$$\text{MSE} = \frac{1}{\text{PQ}} \sum_{i=1}^{\text{P}} \sum_{j=1}^{\text{Q}} [\text{O}(i, j) - \text{W}(i, j)]^2$$

$$\text{PSNR} = 10 \log (\max(f(i,j)^2)/\text{MSE}$$

Correlation represents the similarity between the two images i.e., embedded image and source or extracted image. Correlation between two images are computed using the following equation.

$$\text{Corr}(w, \text{E}) = \frac{\sum_{i=1}^{\text{N}} w_i \text{E}_i}{\sqrt{\sum_{i=1}^{\text{N}} w_i^2 \sum_{i=1}^{\text{N}} \text{E}_i^2}}$$

Table 1
PSNR computation between the original frame and the extracted frame in case of distorted video

Frame No	*DWT-SVD*	*DCT-SVD*	*Proposed*
10	52.86	52.136	53.25
20	52.81	52.891	52.975
30	52.155	52.119	53.076
40	52.498	52.128	53.65
50	52.187	52.113	53.721
60	52.353	52.535	53.986
70	52.652	52.832	53.156
80	52.751	52.715	53.585
90	52.397	52.877	52.898
100	52.733	52.183	52.9876

The PSNR values for the traditional watermarking models and the proposed model are tabulated in Table1. The PSNR for all the models are well acceptable level. Also, the average PSNR for the entire big video file was found out to be 53.39 dB which are well acceptable value.

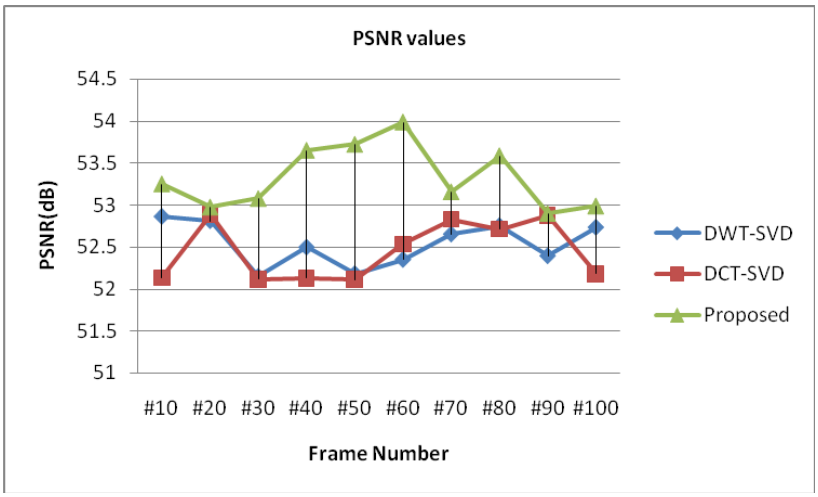


Figure 7: PSNR computation between the original frame and the extracted frame in case of distorted video.

The PSNR values for the traditional watermarking models and the proposed model are shown in Figure 7. The PSNR for all the models are well acceptable level. Also, the average PSNR for the entire big video file was found out to be 53.39 dB which are well acceptable value.

Table 2
Correlation computation between the original frame and the extracted frame in case of distorted video

Frame No	*DWT-SVD*	*DCT-SVD*	*Proposed*
#10	0.673	0.713	0.729
#20	0.683	0.675	0.731
#30	0.657	0.698	0.75
#40	0.673	0.713	0.725
#50	0.682	0.561	0.691
#60	0.636	0.626	0.682
#70	0.619	0.604	0.783
#80	0.735	0.548	0.813
#90	0.716	0.691	0.862
#100	0.722	0.638	0.793

From the Table 2, it can be observed that the correlation of the proposed model is found to have good correlation compared to the traditional video watermarking models.

4. CONCLUSION

In this paper, the PSNR obtained is higher and the correlation computation of the proposed model is found to be better than the traditional video watermarking models. Also geometric transformations such as rotation, scaling and compression of video frames may be due to image corruption and video compression modes. In the traditional video watermarking models, watermark can be embedded either to compressed data or uncompressed data. This paper proposes a novel chaotic hash based video watermarking model for video protection and authentication. In this model, we have proposed a novel chaotic hash algorithm on video compression video files to speed-up the watermark embedding and extraction process. Experimental results show that proposed model has high computation speed and accuracy compared to traditional compressed video watermarking models. In future, this work can be extended to web based video watermarking process on the video streaming applications.

REFERENCES

[1] Yen, S. H., Chang, H. W., Wang, C. J., Wang, P. S., & Chang, M. C. (2008, December). A scene-based video watermarking technique using SVMs. In*Pattern Recognition, 2008. ICPR 2008. 19th International Conference on* (pp. 1-4). IEEE.

[2] Facciol, R., & Farrugia, R. A. (2010, December). Robust video transmission using reversible watermarking techniques. In *Multimedia (ISM), 2010 IEEE International Symposium on* (pp. 161-166). IEEE.

[3] Fung, C. W. H., & Godoy Jr, W. (2011, September). A new approach of DWT-SVD video watermarking. In *2011 Third International Conference on Computational Intelligence, Modelling & Simulation* (pp. 233-236). IEEE.

[4] Prathik, P., Krishna, R., Nafde, R. A., & Shreedarshan, K. (2013, January). An Adaptive blind video watermarking technique based on SD-BPSO and DWT-SVD. In *Computer Communication and Informatics (ICCCI), 2013 International Conference on* (pp. 1-6). IEEE.

[5] Biswas, S. N., Hasan, T., DasGupta, S., Das, S. R., Groza, V., Petriu, E. M., & Assaf, M. H. (2013, May). Compressed video watermarking technique. In *2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)* (pp. 1790-1794). IEEE.

[6] Aniyan, A., & Deepa, J. (2013). Hardware implementation of a robust watermarking technique for digital images. In *2013 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*.

[7] Rawat, C. D., & Shivamkutty, S. M. (2014, August). Digital watermarking of video using hybrid techniques. In *Advances in Communication and Computing Technologies (ICACACT), 2014 International Conference on* (pp. 1-5). IEEE.

[8] Walia, E., & Suneja, A. (2014). A robust watermark authentication technique based on Weber's descriptor. *Signal, Image and Video Processing*, *8*(5), 859-872.

[9] Alenizi, F., Kurdahi, F., Eltawil, A., & Aljumah, A. (2015, December). DWT-based watermarking technique for video authentication. In *2015 IEEE International Conference on Electronics, Circuits, and Systems (ICECS)* (pp. 41-44). IEEE.

[10] Patil, R. D., & Metkar, S. (2015, August). Fragile video watermarking for tampering detection and localization. In *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*(pp. 1661-1666). IEEE.

[11] PM, N., & Bijlani, K. (2015, September). Copyright Protection for E-Learning Videos Using Digital Watermarking. In *2015 Fifth International Conference on Advances in Computing and Communications (ICACC)* (pp. 447-450). IEEE.

[12] Shelke, N. A., & Chatur, P. N. (2016, March). Optimized and hybrid based watermarking system for digital video security. In *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*(pp. 1068-1074). IEEE.

[13] Kadu, S., Naveen, C., Satpute, V. R., & Keskar, A. G. (2016, March). A blind video watermarking technique for indoor video content protection using Discrete Wavelet Transform. In *Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference on* (pp. 1-6). IEEE.