Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1327–1339
DOI : 10.47974/JDMSC-1748

Robust video watermarking algorithm based on motion frames and encryption

Praful Saxena *
Department of Computer Science and Engineering
Maharishi University of Information Technology
Lucknow
Uttar Pradesh
India

Santosh Kumar †
Department of Computing and Engineering
Galgotia University
Greater Noida
Uttar Pradesh
India

Abstract

Rapidly growing technologies over the internet are used to transfer digital media content at a high rate nowadays. The growth in these technologies results in the creation of identical copies of original multimedia data easily. The creation of these identical copies states the false claim of the ownership of digital media by any malicious user. The proposed method suggests protecting these types of the false claim by inserting a watermark into selected motion frames. Before embedding the watermark, it is scrambled by using an algorithm having a secret key. With help of this key, the scrambled watermark will be reconstructed whenever it is required. With the help of DWT method along with using SVD technique watermark is inserted into the selected frame from the original media. The results of the proposed algorithm show that the scheme is secure and robust against different types of attacks whether it is intentional and unintentional. The proposed scheme is found more secure for the protection of false claims of malicious users over digital media.

Subject Classification: *68U10 Computing methodologies for image processing.*

Keywords: *Ownership protection, Wavelet transform, Motion frames, SVD, Video watermarking.*

* *E-mail:* **shyam.praful@gmail.com (Corresponding Author)**
† *E-mail:* **sant.7783@hotmail.com**

1. Introduction

The higher growth in the internet bandwidth makes it easily possible to share multimedia data over various devices. This high order sharing reduces the possibility of security of digital media content. The advancement of technology related to multimedia content introduces lots of issues like ownership, authentication of content, copyright protection, and many more. Tempering with digital media is one of the major concerns related to the copyright protection of media. Proper solutions should be developed to protect the media from such unauthorized user access. The use of cryptography enables the protection of media content during transmission. The malicious user cannot access or modify the media content without knowing the encryption key. The scheme associated with the cryptographic approach encrypts the data at the authorized user end and at the end of the receiver the data will be decrypted which results in the original data. Therefore a secure and robust scheme needs to be developed to avoid illegal media reproduction and false claims of digital media content. The advent of watermarking schemes gives a feasible solution for such problems having some challenges still to be faced.

Digital Watermarking is a feasible scheme in which additional information is hidden into host media content having a relation between both of them. Digital watermarking can be applied to audio, video, and image. Watermark is used proof copyright protection by embedding the watermark into the real source video and after that extraction process is performed which results from the same watermark which was extracted. In the process of digital watermarking proper balanced tradeoff should be maintained among payload, robustness, and perceptibility. In the watermarking method, the extraction process can only be performed by an authorized user only in the case to prove copyright protection. The scheme used to embed the watermark should maintain robustness so that embedded information should not be destroyed by any malicious use [1]. In case to select the type of watermark we can consider any gray level image, name, logo any timestamp, etc. These types of watermark are frequently used in various watermark implementation techniques. In the present scenario of the market, various types of video content are available like advertisements, training videos, workshop videos, games, etc. The video objects are categorized as real source video and compressed video. During the implementation of the same, the balanced trade-off among watermarking features should be balanced. Any malicious user can try to modify the video content by performing some kind of attack. Attacks can be categorized as geometric attacks, cropping, resize, and rotation attacks[2]. Another category of attacks performed on the image is image enhancement like histogram equalization, histogram processing, noise removal, frame restoration, contrast enhancement, and many more. In the video, media attacks are intentional and unintentional specific attacks. Any malicious user can insert the video frame or some clip of video are cut down from the real source video content[3]. Such kind of attacks comes under the category of unintentional attack. The replacement of frames comes under intentional attacks. During the implementation of the watermarking scheme, the perceptibility should be maintained up to a minimum threshold value. Another consideration is to maintain the payload capacity which states that the amount of information to be embedded into the host file.

2. Methodology Used

2.1 *Discrete Wavelet Transform*

Discrete Wavelet transform is the kind of mathematical tool that is used to implement wavelet transform. It uses the discrete set of wavelet scales having some defined rules. the Wavelets are the mathematical tool that is used to change the coordinate system as per the need. The original signal is broken down into a series of wavelets by the wavelet transform, which differs from a continuous wavelet transform[4]. The construction of the wavelet can be done from a scaling function which describes the scaling properties of an object. The layer having more resolution states that it contains more information about the object like an image. The wavelet results in the natural multi-resolution image having all the important edges of the image. Its generation and calculation of DWT are well suited to the digital computer[5]. If an image is passed through the DWT function then it is a sum of the wavelets having different locations and scales. DWT represents the image into high pass and low pass coefficients. In this, the image is passed through the high and low filters. When the image is passed through the DWT then the analysis filter is used to separate the image into various frequency bands. The analysis filters separate the image into four sub-bands LL, LH, HL HH. It is also called the first level of decomposition and it also represent the finer scale coefficients. The various level of decomposition depends on the need of the application implementation. In most of the watermarking methods the decomposition is done up to 3 level. The multi resolution concept is a conceptual concept

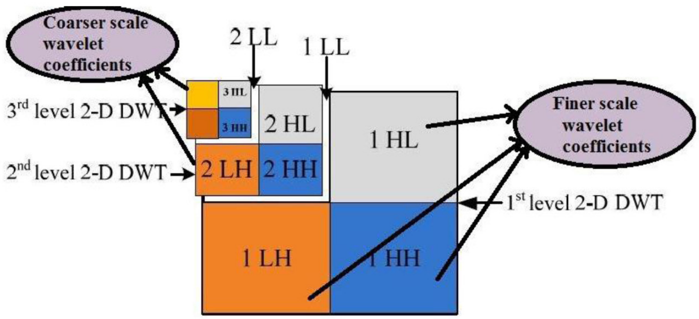

Figure 1
3Level DWT

that shows the signals that will be decomposed into fine details and finer approximations. The finer details subspaces are represented by a coarse and finer approximation. One of the major benefit for using the Discrete Wavelet Transform method is its excellent spatio-frequency localization property[6]. DWT is used by many watermarking algorithm for the copyright protection due to the imperceptibility property also[7].

2.2 *Singular Value Decomposition*

Singular value decomposition is a linear algebra mathematical tool which is used for the purpose of factorization of a real or complex matrix[8].SVD tool performs the decomposition of square matrix into ant m x n matrix with the extension polar decomposition. When SVD is applied on any m x n complex or real matrix M than it will be factorized into the form of $U\Sigma V^*$ where U is defined as the real or complex unitary matrix of the order m x m. Σ is defined as the rectangular matrix having non negative numbers on the diagonal and its order is m x n. V is defined as the real or complex unitary matrix having order of n x n. The diagonal entries are called the singular values of matrix M[9].

3. Literature Review

The fast motion frame to embed the watermark into video object. Author converts the fast frame RGB to YCbCr color space and after that the frame gets transformed into 1-level decomposition of MR SVD. SVD is applied on each block approximation which provides robustness to the algorithm. The algorithm is tested against various attacks and the Watermark is extracted from the video object having a satisfied perceptibility[10]. The various applications of watermarking and its design features. Authors describes the implementation schemes which are categorized in spatial domain and frequency domain. A scheme to extract the watermark from the distorted video by using distortion model based on barrel. After applying the attacks the watermark calculated is by means of correlation and mean square error to find the accuracy of watermark signal[11]. The use of scrambled watermark for the implementation of watermarking over video object. Author uses un-encoded video to measure the security of the algorithm.Generalized Multi stage Arnold scheme is used to scramble the watermark. Scrambling the watermark improves the security feature of the algorithm. Author implements the watermarking process by selecting the U component from the YUV model. Proposed algorithm gives a good quality to the video object after embedding[12]. To avoid accidentally embedding the watermark in all the video frames, we only use the frames with big motion energy to embed it. This method works since the human visual system can't detect the details of fast moving regions. The algorithm is focused on the classification of blocks and shot segmentation. The watermark is computed as a small image that is proportional to the size of the host image. It is then embedded into the selected frames[13].

Discrete Wavelet Transform (DWT), Hessenberg Decomposition (HD), and Singular Value Decomposition (SVD) are the foundations of the watermarking method proposed in this research, which is enhanced by the Firefly Algorithm (FA). The suggested method makes the approach blind by using Hu's invariant moments, which are resistant to attacks that rotate, scale, and translate (RST) the image. The watermark is undetectable in the final watermarked image, making it appropriate for a broad range of watermarking applications. The suggested method involves applying a 2 Level DWT to a given colour image to separate it into the LL, LH, HL, and HH bands. These HH band coefficients are used as HD's input. To create the U, S, and V matrices, the output is placed through an SVD process. The Hu's unchanging values are scaled and transformed into binary strings using logarithm scaling. The binary matrix corresponding to the binary watermark is periodically XoRed with the same values to produce a new binary matrix with an identical dimension as the count of 2X2 partitions of S. Through altering the orthogonal V matrices, the watermark is embedded. The Firefly technique is used to calculate the change's size while taking robustness and imperceptibility into account as trade-off characteristics[14]. A robust image steganography method for sharing photos on social networks is presented in this paper and is based on graph signal processing. We first used quantum scrambling to obtain a scrambled version of the secret image for the embedding. The cover image and scrambled secret image were then both subjected to graph wavelet processing, which was followed by (alpha) merging on both image signals (cover image signal and scrambled image signal). The generated image was then subjected to an inverse graph wavelet modification to produce the stego image. This study used graph wavelet treatment to enhance interpixel correlation, which led to both the extracted secret image and the stego image having great visual quality[15]. The generated image is subjected to the GSP-based inverse wavelets to produce the stego image. As illustrated in the simulation results, the application of GSP in this case improves inter-pixel correlation, leading to superior visual quality stego and derived secret image[16].

4. Watermark Encryption and Frame Extraction

The logic behind the encryption of watermark is to provide the security to embedded video object. The encryption will be done during the embedding and decryption will be done during the extraction of watermark. Secret key is generated for this purpose.The benefit of encryption mechanism is that the cipher image is not logically readable by the any user. The watermark will be in a state of readable after decrypting it with the secret key. Appropriate algorithm[2] proposed by author is found a strong algorithm for encrypting the watermark.Initially we decide the key used for scrambling the watermark which will be as follows: K={1 6,1,14,3,12,5,10,7,8,9,6,11,4,13,2,15}. Key is a arrangement of even and odd numbers which will be used to scrambling the watermark. The size of the watermark will be same as of the video object. The watermark is portioned and the again rearranged as per the decided value K. This process results the encryption process of watermark. Figure 2 shows the original watermark and Figure 3 shows some parts of the scrambled watermark.

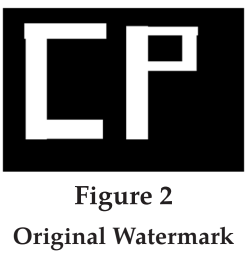

Figure 2

Original Watermark

Figure 3

Scrambled Watermark

After the scrambling of watermark the next step is to extract the motion frames from real source video object. The motionless area of the video object is not robust and it is a comparatively easy task to exploit on the motionless frames based watermarking method. After execution of proposed process 14 frames are found which were based on the motion from the coastguard video object. The threshold value is set upto 5000 to extract the frames. The proposed scheme embed the scrambled watermark into the frame which results that few frames are get watermarked instead of all. It is also observed that quality of watermarked video also maintained.

Figure 4

Sample Extracted frames from Video

5. Proposed Watermarking Scheme

5.1 *Watermark Embedding*

The algorithm for inserting the scrambled watermark is implemented by embedding the encrypted part of watermark into motion frame.If the selected frame is not a motion frame than no embedding process will be

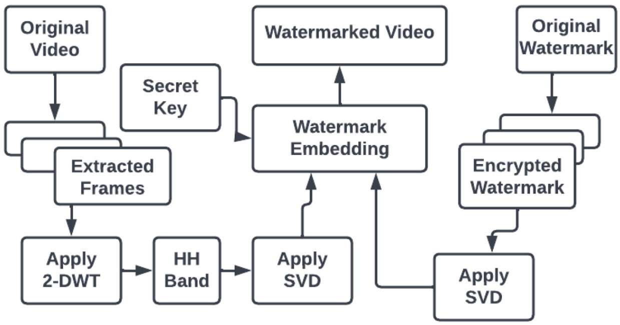

Figure 5

Watermark Embedding Flow Chart

executed. The embedding process done only on motion frames. If the count of extracted motion frames is more than the encrypted parts of watermark than repeat the sequence of encrypted watermark from one. Now transform motion frame into various luminance components. After the conversion, discrete wavelet transformation is executed up to 2-Level which results in four sub bands LL, LH, HL, HH. The HH band is used for the insertion of watermark. Apply the SVD method on this band which results the matrix of three components from which diagonal matrix is used insert the watermark. SVD method is also applied on watermark and diagonal matrix is used for watermarking purpose. The embedding of watermark is executed by following equation-

$$SVD_{WD} = SVD_{Y} + \alpha SVD_{W} \quad (1)$$

SVDY is the diagonal matrix of Y component after the apply SVD operation on it. SVDw represents the diagonal matrix of scrambled watermark.The value of α will be 0.01. After performing the watermarking operation the resultant diagonal matrix is SVDWD which is watermarked frame. After the insertion of watermark on all frames the watermarked video is generated which leads the final watermarked video. Figure 5 shows the flowchart of the proposed method for watermark embedding.

5.2 *Watermark Extraction*

The Extraction process is required when we need to extract the watermark which is inserted into motion frame. For this extract the adjacent RGB frame from the watermarked video and evaluate that if it is motion frame. If it is a motion frame than it must contain a watermark in it. Apply the process which results RGB frame into three different

Figure 6

Original Video

Figure 7

Watermarked Video

Figure 8

Original Video

Figure 9

Watermarked Video

components stated as Y, Cb and Cr. Now apply DWT of 2 level and select HH band. Apply SVD method to find the diagonal matrix which is singular values. The singular values of watermark is generated by given mathematical formula

$$S_{w'} = (S_o - S_w)/\alpha \tag{2}$$

Here Sw and So represents the singular values of the frame which is extracted from the real source video and watermarked video frame. Now repeat this process to obtain all the watermark and then the final watermark is generated. The estimated watermark can be generated as-

$$Watermark = UW * SW' * VW \tag{3}$$

UW and VW are the orthogonal matrix of watermark. These values are referred as the values of original watermark.The embedding algorithm is performed on two videos. Figure 6 and Figure 7 are the original video and watermarked video. Figure 8 and Figure 9 are the result of embedding process on another video.

6. Experimental Results

After the extraction of watermark , two major characteristics are to be checked one is robustness of algorithm and perceptibility.For the result processing various attacks are applied on watermarked video and then the extraction process is implemented. PSNR is tool used for the measurement of the perceptibility. The unit of PSNR is dB. The features of video are investigated in order to assess the suggested watermarking scheme's durability. Various attacks are executed on the watermarked video to destroy the watermark inserted in real video object. The proposed is found robust against defined attacks above. The evaluation is carried by analyzing the original watermark and driven out watermark by observing NC. The table shown below is the level of sturdiness of proposed algorithm. The proposed algorithm is applied on two videos foreman.avi and akiyo. avi. The applied attacks mentioned above measure the robustness of the algorithm.

Table 1

Proposed Algorithm Robustness Results (Foreman.avi)

S.No	Attack Performed	NC	PSNR
1.	Speckle Noise	0.881	40.2414
2.	Frame Deletion (around 10%)	0.908	38.1008
3.	Rotation	0.893	47.0024
4.	Gaussian Low Pass Filter	0.811	42.2003
5.	Cropping	0.898	37.8870
6.	Salt and Pepper	0.882	41.2404

Table 2

Proposed Algorithm Robustness Results (akiyo.avi)

S.No	Attack Performed	NC	PSNR
1.	Speckle Noise	0.902	39.0047
2.	Frame Deletion (around 15%)	0.911	38.0021
3.	Rotation	0.901	41.2414
4.	Gaussian Low Pass Filter	0.806	43.5724
5.	Cropping	0.885	40.0122
6.	Salt and Pepper	0.917	41.2141

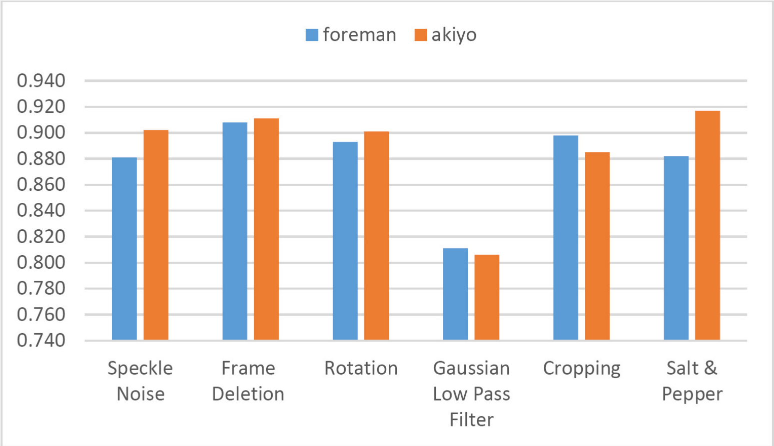

Figure 10

Result Comparison(NC Values) on foreman and akiyo video

The post extraction method shows that the extracted watermark has robust values of NC,PSNR with respect to several attacks.Table 1 and Table 2 shows the values of NC and PSNR and these values shows the robustness of the proposed method against several attacks. Figure 10 shows comparison on the two video oblects on which the proposed method id implemented.

7. Conclusion

The quality of the proposed scheme is that it manages to maintain the robust ness against attacks, video specific attacks. The security proposed in the algorithm is implemented at 2-layer security. The watermark is encrypted before the process of embedding and further it is segmented into sub images by extracting the motion frames from real source video object. Total number of frames in video object is 300 but only very few of the frames have gone through the process of embedding which improves the quality of video after embedding. After using the suggested algorithm, it was discovered that there was no similar visual gap between the watermarked and original source videos, indicating that the watermark's quality was sufficient in terms of imperceptibility. Because the real inserted watermark and real source video are provide whenever the extraction phase is executed, such resulting watermarking technique is ideal for applications which are private in nature. The greater robustness should be tested for composite assaults, collusion attacks, ambiguity attacks, algorithms should also be designed for video watermarking which are in blind category , according to future studies.In the blind video watermarking there is no requirement of real source video and original watermark for the extraction of embedded watermark.

References

[1] Q. Li and E. C. Chang, "Zero-knowledge watermark detection resistant to ambiguity attacks," in *Proceedings of the Multimedia and Security Workshop 2006, MM and Sec'06*, 2006, Vol. 2006, doi: 10.1145/1161366.1161395.

[2] R. Ahuja, Purnima, M. J. Haque, S. Tanwar, N. Gautam, and A. Rana, "Secure and Robust Watermarking Scheme based on Motion Features for Video Object," (2020), doi: 10.1109/ICRITO48877.2020.9197967.

[3] N. Chawla and V. Singh, "A novel video watermarking scheme based on DWT and PCA," *Int. J. Eng. Adv. Technol.*, Vol. 7, No. 5, (2018).

[4] L. Agilandeeswari and K. Ganesan, "A robust color video watermarking scheme based on hybrid embedding techniques," *Multimed. Tools Appl.*, Vol. 75, No. 14 (2016), doi: 10.1007/s11042-015-2789-9.

[5] Z. S. Veličković, Z. N. Milivojević, and M. Z. Veličković, "A secured digital video watermarking in chrominance channel," in *2018 23rd International Scientific-Professional Conference on Information Technology, IT 2018* (2018), vol. 2018-January, doi: 10.1109/SPIT.2018.8350858.

[6] A. A. Mohammed, D. A. Salih, A. M. Saeed, and M. Q. Kheder, "An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique," *Multimed. Tools Appl.*, Vol. 79, No. 43-44 (2020), doi: 10.1007/s11042-020-09694-9.

[7] M. Shanmugam and A. Chokkalingam, "Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method," *Microsyst. Technol.*, Vol. 24, No. 12 (2018), doi: 10.1007/s00542-018-3870-x.

[8] H. A. Abdallah, M. M. Hadhoud, and A. A. Shaalan, "SVD-based watermarking scheme in complex wavelet domain for color video," (2009) doi: 10.1109/ICCES.2009.5383220.

[9] G. G. & R. Kumar, "Analysis of image types, compression techniques and performance assessment metrics : A review," *J. Inf. Optim. Sci.*, Vol. 43, No. 3, p. 8 (2022).

[10] A. D. & M. N. Mohanty, "Transformation of 1-D data to 2-D image using stochastic mapping method for secured skin lesion detection," *J. Inf. Optim. Sci.*, Vol. 43, No. 8, p. 8 (2022).

[11] M. K. G. & S. R. D. Apoorva Katyayan, Ajay Khunteta, "Detection of copy-move image forgery using normalized cross correlation and fast fourier transform," *J. Stat. Manag. Syst.*, Vol. 22, No. 4, p. 10, (2019).

[12] K. Meenakshi, K. Swaraja, and P. Kora, "A robust DCT-SVD based video watermarking using zigzag scanning," in *Advances in Intelligent Systems and Computing*, Vol. 900 (2019), doi: 10.1007/978-981-13-3600-3_45.

[13] R. Naskar and R. S. Chakraborty, "Reversible Digital Watermarking: Theory and Practices," *Synth. Lect. Inf. Secur. Privacy, Trust*, Vol. 5, No. 1, (2014), doi: 10.2200/s00567ed1v01y201401spt010.

[14] M. M. Sachin Sharma, Shikha Choudhary, Vijay Kumar Sharma, Ankur Goyal, "Image Watermarking in Frequency Domain using Hu's Invariant Moments and Firefly Algorithm," *I.J. Image, Graph. Signal Process.*, Vol. 14, No. 2, pp. 1-15 (2022).

[15] V. K. Sharma, P. C. Sharma, H. Goud, and A. Singh, "Hilbert quantum image scrambling and graph signal processing-based image steganography," *Multimed. Tools Appl.*, Vol. 81, No. 13, (2022), doi: 10.1007/s11042-022-12426-w.

[16] V. K. Sharma, D. K. Srivastava, and P. Mathur, "Efficient image steganography using graph signal processing," *IET Image Process.*, Vol. 12, No. 6, (2018), doi: 10.1049/iet-ipr.2017.0965.