International Journal of Advances in Engineering & Technology, July 2012.
©IJAET **ISSN: 2231-1963**

A CHAOS ENCRYPTED VIDEO WATERMARKING SCHEME FOR THE ENFORCEMENT OF PLAYBACK CONTROL

K. Thaiyalnayaki and R. Dhanalakshmi

Assistant Professor, Department of Information Technology, Sri Venkateswara College of Engineering, Pennalur, Sriperumbudur, India.

ABSTRACT

The ability to make perfect copies of Digital content and the ease by which copies can be distributed facilitate misuse, illegal distribution, plagiarism, misappropriation. It is a problem of Digital Rights Management (DRM) systems aiming at protecting and enforcing the legal rights associated with the use of digital content distributed . A watermarking scheme that discourages video piracy through the prevention of video playback is presented as a solution. In this method, the video is watermarked so that it is not permitted to play if a video player detects a watermark that is not extracted properly. Procedure takes the advantage of the properties of compression techniques like Robust Discrete Wavelet Transform and Singular Value Decomposition to provide Imperceptibility, Compression and Robustness to the created watermark which can withstand intentional attacks such as frame dropping, frame averaging and geometric distortions like rotation, scaling, cropping and lossy compression. The proposed work also uses chaos encryption for ensuring security. The objective of the scheme is to exploit the characteristics of the compression techniques and the algorithm for the creation of a robust watermark which is then used for making a video secure. This paper proposes an innovative, invisible watermarking scheme for copyright protection of digital content with the purpose of defending against digital piracy.

KEYWORDS: *Video Piracy, Access Control, Singular Value Decomposition, Chaos Encryption.*

I. INTRODUCTION

The practice of copying and selling copyrighted information without proper rights, a great concern to original content creators is termed as Piracy. The owner of the digital content, desires to ensure that all access to the content is authorized under the rules of a license (conditional access), unauthorized reproductions cannot be easily made (copy protection), and any illegal copies that are created can be detected and traced (authentication and content tracking). An ideal solution to this problem would be to somehow integrate the security information directly into the content of the multimedia document, such that the security information should be inseparable from the document during its useful lifespan. Moreover, the additional information should be perceptually invisible as the multimedia documents are ultimately processed by human viewers or listeners and the contents should not be affected. Watermarking provides the desired solution.

The paper is organized as follows: Section I deals with watermarking, Section II on existing work, Section III on proposed work followed by experimental results and conclusion.

1.1 WATERMARKING

The process of embedding information into another object/signal can be termed as watermarking. Watermarking is mainly used for copy protection and copyright-protection. Historically, watermarking has been used to send sensitive information hidden in another signal. Watermarking has its applications in image/video copyright protection. The characteristics of a watermarking algorithm are normally tied to the application it was designed for [2].

The first applications were related to copyright protection of digital media. In the past duplicating artwork was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights, artists of today can watermark their work by hiding their name within the image. Hence, the embedded watermark permits identification of the owner of the work.

II. EXISTING WORK

2.1.1 Introduction

Wavelet transforms have gained widespread acceptance in signal processing been represented in the form of wavelets which are wave like oscillation with an amplitude. When researchers took this part of digital signal processing technique to the image processing field, they found considerable results. This resulted in wavelet compression which is a form of data compression where the goal is to store the image data in as little space as possible in a file. Wavelet compressions can be both lossless and lossy. The method for compression follows the wavelet transform where pixels of a complaint image are been transformed into respective coefficients. This produces as many coefficients as there are pixels in the image. These coefficients can then be compressed more easily because the information is statistically concentrated in just a few coefficients. This principle is called transform coding. Because of their inherent multi-resolution nature, wavelet coding schemes are especially suitable for watermarking where scalability and tolerable degradation are important [4]. Some of the commonly used transforms are Continuous Wavelet Transform (CWT) and Discrete Wavelet Transform (DWT). Complex wavelets have also been employed to create watermarks that are robust to geometric distortions. The complex wavelet transform is an over complete transform and, therefore, creates redundant coefficients but it also offers some advantages over the regular wavelet transforms. The existing work uses such a complex wavelet transform in two trees and is briefly explained.

2.1.1 The Dual Tree Complex Wavelet Transform

This transform is a variation of the original DWT with the main difference being that it uses two filter trees instead of one. For a 1-D signal, the use of the two filter trees results in twice the number of wavelet coefficients as the original DWT. The coefficients produced by these two trees form two sets that can be combined to form one set of complex coefficients [4] [5].

The watermark is a pseudorandom sequence of 1's and 0's. It is created using a key which a constant (positive integer) is provided by the user. The use of the beta symbol for consecutive frames offers some robustness to temporal synchronization attacks. To provide more robustness to lossy compression, the watermark will be embedded in the coefficients of higher decomposition levels. In the implementation, the watermark is embedded in levels 3 and 4 of 4-level Dual Tree Complex Wavelet Transform decomposition [6].

2.1.2 Limitations of the existing work

The transformation technique which is used here reproduces the frame into the wavelet domain as a matrix of complex coefficients that are used then to construct the whole digital material which costs much of memory space. The existing work uses key as a watermark which is prone to attacks thereby breaking the same and thus the watermark. Frame dropping and frame averaging are some important intentional

attacks that are not dealt with. The existing work is more limited to the creation of the watermark, embedding into frames and checking it's robustness by passing it to some geometric distortions like cropping and scaling.

III. PROPOSED WORK

3.1 Objective

The objective of the proposed work is to use the watermark for the purpose of security by encoding the same into the video frames and blocking access to media content if the decoding is not done with the right inverse procedures. Also making the scheme more robust by subjecting it to attacks and evaluating the performance is proposed. The proposed work uses two compression techniques and a scrambling algorithm to construct the robust and secure watermark.

Techniques and algorithms used

3.1.1 Discrete Wavelet Transform

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. Wavelets are special functions which, in a form analogous to sine and cosine in Fourier analysis, are used as basal functions for representing signals [2]. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency and location information in time [3][5].

It converts an input series x_0, x_1, ..x_m, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series (of length n/2 each) given by the equations 3.1 and 3.2.

$$H_i = \sum_{m=0}^{k-1} x_{2i-m} \cdot s_m(z) \quad (3.1)$$

$$L_i = \sum_{m=0}^{k-1} x_{2i-m} \cdot t_m(z) \quad (3.2)$$

Where $s_m(Z)$ and $t_m(Z)$ are called *wavelet filters*, K is the length of the filter, and I=0, ..., [n/2]-1.

3.1.1.1 Advantages of DWT

Allowing good localization, both in time and spatial frequency domain, DWT is well known transformation. The whole image introduces inherent scaling, better identification of which data is relevant to human perception and higher compression ratio, offering higher flexibility. (64:1 vs. 500:1).

3.1.2 Singular value decomposition

This compression technique comes from the applied theory of linear algebra and is called "singular value decomposition (SVD)". SVD method can transform matrix A into product USV^T , which allows us to refactoring a digital image in three matrices[1]. The use of singular values of such refactoring allows us to represent the image with a smaller set of values, which can preserve useful features of the original image, but use less storage space in the memory, and achieve the image compression process. The experiments with different singular value are performed, and the compression result was evaluated by compression ratio and quality measurement [3] [7].

3.1.2.1 Process of Singular Value Decomposition

Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra by many renowned mathematicians.
SVD has many practical and theoretical values; Special feature of SVD is that it can be performed on any real (m, n) matrix. Let's say we have a matrix *A* with *m* rows and *n* columns, with rank *R and* $R \leq n \leq m$. Then the *A* can be factorized into three matrices: $A = USV^T$ (See the figure 1 below for illustration)

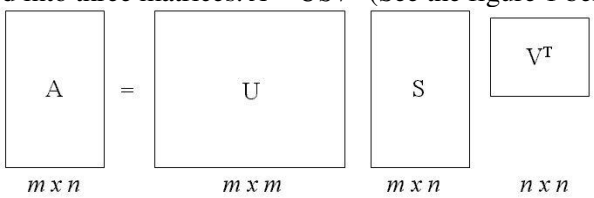

Figure 1. General SVD manipulation matrices

Let A be a general real matrix of order m × n. The singular value decomposition (SVD) of A is the factorization:
$A = U * S * V^T$
Where U and V are orthogonal (unitary) and S = diagonal (σ_1, σ_2, ..., σ_r), where σ_i, i = 1(1)r are the singular values of the matrix A with r = min(m, n) and satisfying
$\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_r$
The first r columns of V the right singular vectors and the first r columns of U the left singular vectors [7].

3.1.2.2 Properties of SVD

There are many properties and attributes of SVD; here we just present parts of the properties that we are going to use in this work.
1. The singular value σ_1, σ_2... σ_n are unique, however, the matrices *U* and V are not unique.
2. Since $A^T A = VS^T SV$, so *V* diagonalizes $A^T A$, it follows that the **v***j* s are the Eigen vectors of $A^T A$.
3. Since $AA^T = USS^T U^T$, so it follows that *U* diagonalizes AA^T and that the *i* u's are the eigenvectors of AA^T.
4. If *A* has rank of *r* then v_j, v_j, …, v_r form an orthonormal basis for range space of A^T, $R(A^T)$, and u_j, u_j, …, u_r form an orthonormal basis for range space *A*, *R*(*A*).
5. The rank of matrix A is equal to the number of its nonzero singular values.

3.1.2.3 SVD Approach for Image Compression

Image compression deals with the problem of reducing the amount of data required to represent a digital image. Compression is achieved by the removal of three basic data redundancies: 1) Coding redundancy, which is present when less than optimal; 2) Inter pixel redundancy, which results from correlations between the pixels; 3) Psycho visual redundancies, which is due to data that is ignored by the human visuals [3].
When an image is SVD transformed, it is not compressed, but the data take a form in which the first singular value has a great amount of the image information. With this, we can use only a few singular values to represent the image with little differences from the original [1].
To measure the performance of the SVD image compression method, we can compute the compression factor and the quality of the compressed image. Image compression factor can be computed using the Compression ratio (CR). Equation 3.3 is used for calculating CR.

$$CR = m*n/ (k (m + n + 1)) \quad (3.3)$$

To measure the quality between original image *A* and the compressed image *k A,* the Measurement of Mean Square Error (MSE) can be computed. Equation 3.4 gives MSE value.

$$MSE = \frac{1}{mn} \sum_{x=1}^{m} \sum_{x=1}^{n} (f_A(x,y) - f_{Ak}(x,y)) \quad (3.4)$$

3.1.2.4 Uses of SVD

Use of SVD in digital image processing has advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed. Finally, singular values contain intrinsic algebraic image properties [8]. The singular values are resistant to the following types of geometric distortions:
Transpose: The singular value matrix A and its transpose A^T have the same non-zero singular values.
Flip: A, row-flipped A_{rf}, and column-flipped A_{cf} have the same non-zero singular values.
Rotation: A and A_r (A rotated by an arbitrary degree) have the same non-zero singular values.
Scaling: B is a row-scaled version of A by repeating every row for L_1 times. For each non-zero singular value λ of A, B has $L_1\lambda$. C is a column-scaled version of A by repeating every column for L_2 times. For each nonzero singular value λ of A, C has $L_2\ \lambda$. If D is row-scaled by L_1 times, and column-scaled by L_2 times, for each non-zero singular value λ of A, D has $L_1L_2\lambda$.
Translation: A is expanded by adding rows and columns of black pixels. The resulting matrix A_e has the same non-zero singular values as A.
Overall, the SVD approach is robust, simple, easy and fast to implement. It works well in a constrained environment. It provides a practical solution to image compression and recognition.

3.1.3 Chaos Encryption

Chaos-based image encryption techniques are very useful for protecting the contents of digital images and videos. They use traditional block cipher principles known as chaos confusion, pixel diffusion and number of rounds [12]. The complex structure of the traditional block ciphers makes them unsuitable for encryption of digital images and video[11][13]. Hence chaos encryption is implemented and the algorithm is given as follows:
1.The watermarked image is converted to a binary data stream.
2.A random key stream is generated by the chaos-based pseudo-random key stream generator (PRKG).
3.PRKG is governed by a couple of logistic maps, which is depended on the values of (b, x0,). These values are secreted, and are used as the cipher key.
4.Through iterations, the first logistic map generates a hash value xi+1, which is highly dependent on the input (b, x0), is obtained and used to determine the system parameters of the second logistic map.
5.The real number xi+1 is converted to its binary representation Xi+1, suppose that L=16, thus Xi+1 is {b1, b2, b3, … b16}. By defining three variables whose binary representation is Xl=b1…b8, Xh=b9…b16, we obtain Xi+1'=Xl⊕Xh.
6.Mask the watermarked primary image with the chaos values.

The generator system can be briefly expressed in the following equations:

$$x_{i+1}=bx_i(1-x_i) \quad (3.5)$$

$$x_{i+1}' = X_{i+1}' = X_l \oplus X_h \quad (3.6)$$

$$WI'=WI_i \oplus X_{i+1}' \quad (3.7)$$

3.2 The proposed copyright protection scheme

The proposed scheme contains three phases:

1. Watermark Embedding
2. Watermark Extraction
3. Playback Control

The flow diagrams and the algorithms of the three phases are explained below.

3.2.1 Watermark Embedding Algorithm

The watermark embedding phase uses the transforms and the scrambling algorithms to embed the watermark onto the video frames and in the extraction phase the inverse of the respective transforms and the decoding part of the algorithms are done to extract the watermark [6] [9].

The positioning of these procedures in respective areas deals with real time expertise.

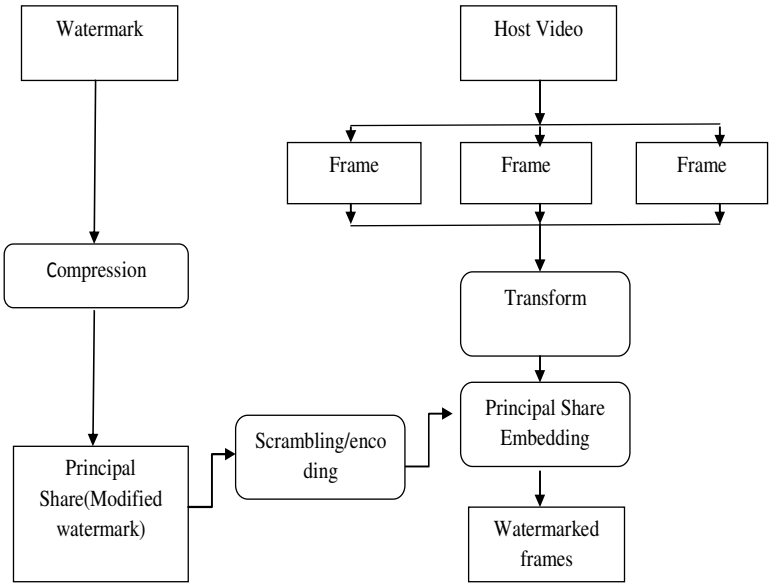

Figure 2. Watermark Embedding Flow diagram

Figure 2 shows the watermark embedding phase where the watermark which is an image is passed into the compression Singular Value Decomposition and the modified watermark (called principal share) is scrambled into the video frames. The video frame is already passed via the transform Discrete Wavelet Transform and the watermark is now embedded into the video frame and the watermarked video frames are the output of the embedding phase [12].
The algorithm first generates the image which is to be used as a watermark and then embeds it to the host video frame for copyright protection, which is described in detail as follows:
Input: The color host video frame $H(N \times N)$, a watermark $W(M \times M)$ and a secret key for scrambling.
Output: The watermarked host video frame.
Step1: The host video is divided into frames.
Step2: The frames thus created are passed into the transform DWT and the transformed frames are obtained.
Step3: The watermark which is an image is compressed by the Singular Value Decomposition procedure and the principal share ie. The modified watermark is obtained.
Step 4: Use Torus-automorphism and the secret key to scramble the watermark into the video frames.
The watermarked video frame and the secret key are then saved for the watermark extraction phase.

3.2.2 Watermark Extraction Algorithm

The extraction algorithm extracts the embedded principal share or the watermark and then reconstructs the watermark for copyright verification.
Input: The suspect video frame $H'(N \times N)$ and the secret key for unscrambling.
Output: The reconstructed watermark WR $(M \times M)$.
Step1: Apply the inverse DWT on each of the suspect video frames H'.
Step2: The inverse of the compression technique SVD is applied to these watermarked video frames obtained in step 1.
Step3: Use Torus-automorphism and the secret key to unscramble the watermark W'.
Step4: Use correction to obtain the corrected watermark.

Step5: Apply reduction to the corrected watermark to obtain the reconstructed watermark *WR*.
Figure 3 shows the reconstruction phase where the inverse of all the algorithms are applied to the suspect or the encoded video frames and the watermark.
The unscrambling is done with the reverse procedure of the scrambling algorithm; the pixels are fine tuned and reduced to extract the watermark. This watermark only if reconstructed, the video is allowed for playback. This is achieved by placing the whole decoding scheme in front of the output buffer.

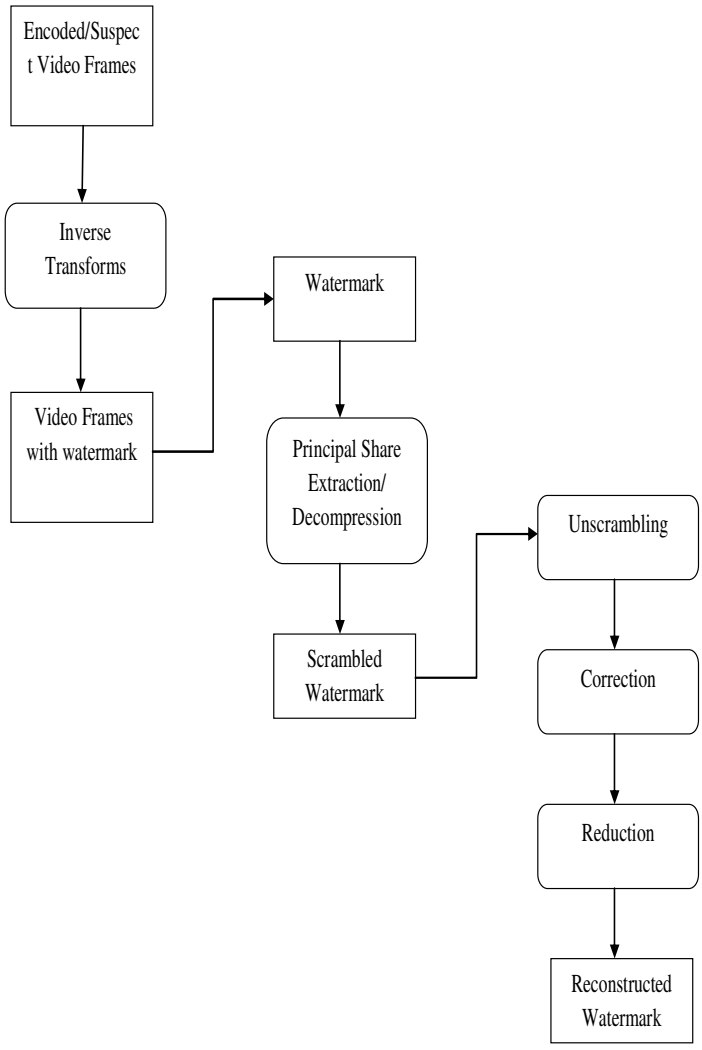

Figure 3. Watermark Extraction Flow diagram

3.2.3 Playback Control Algorithm

The reconstructed watermark becomes the source for letting or preventing the video playback. Only if the frames that are passed to this algorithm contain the correctly reconstructed watermark which is measured by a quantity called the accuracy rate, the video is allowed to play [10].
Step1: The accuracy rate (AR) is calculated for each of the frames..
Step2: If the value of AR is less than one the video is permitted for playing.
Step3: If the value of AR is greater than one the video is not permitted for playing.

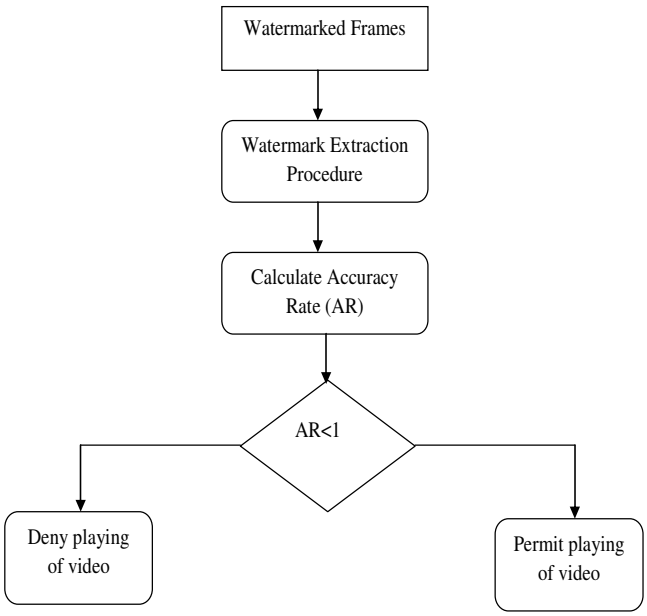

Figure 4. Playback Control Flow diagram

Figure 4 shows the playback control procedure where the video is allowed to play only if the watermark is extracted abiding the rules of the extraction procedure explained earlier and by calculating the measure Accuracy Rate.

IV. EXPERIMENTAL RESULTS

The proposed work is simulated using MATLAB 7.1 and the results are given as follows. Figure 5 shows the result of dividing the input video into frames.

Figure 5. Dividing Video into frames

Figure 6 depicts the watermark used for embedding. The watermark is subjected to SVD for compression.

Figure 6. Watermark Compression using SVD

Figure 7 shows the result after embedding the compressed watermark in the input video.

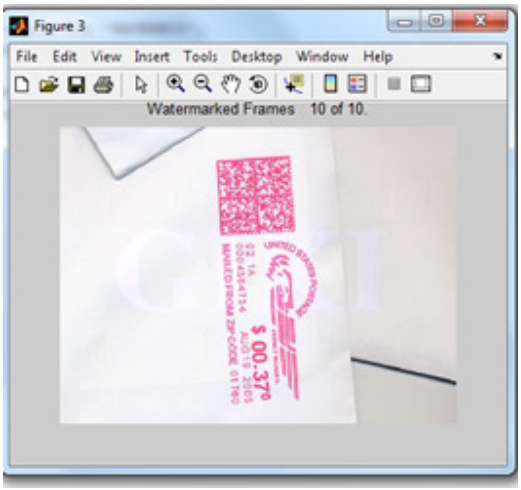

Figure 7. Embedding watermark in the video frame

Figure 8 depicts the watermark which is extracted from the video at the decoder.

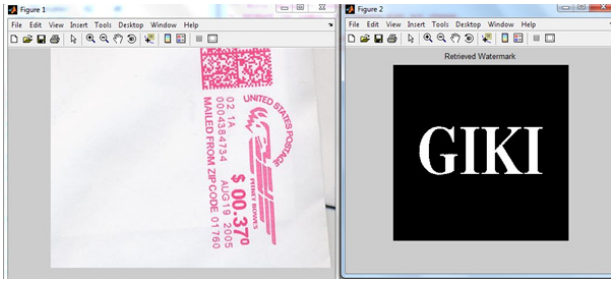

Figure 8. Extracted watermark from the video frame

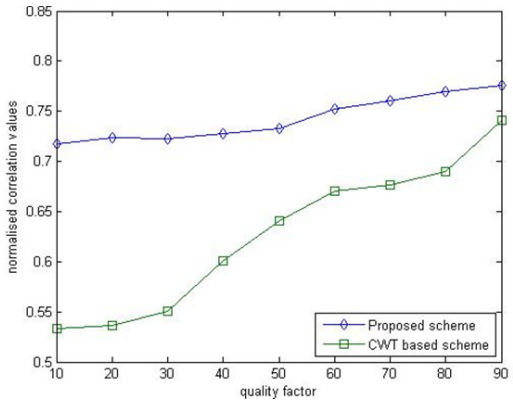

Figure 9. Compression attack on proposed and CWT scheme

Figure 9 shows the comparison between the proposed scheme and an existing benchmark lossy compression attack.

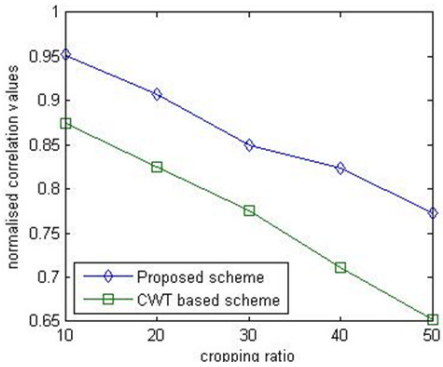

Figure 10. Cropping attack on proposed and CWT scheme

Figure 10 shows the comparison between the proposed scheme and an existing cropping attack [3][8].

The *Accuracy Rate* (*AR*) is used to measure the difference between the original watermark and the recovered one. *AR* is defined as follows:

AR= CP/NP (4.1)

Where *NP* is the number of pixels in the original watermark and *CP* is the number of correct pixels obtained by comparing the pixels of the original watermark to the corresponding ones of the recovered watermark.

V. CONCLUSIONS AND FUTURE WORK

It is a global approach for protecting digital videos that allows the user access to material only in accord with a decoding procedures and algorithms obtained from the creator. The material can be distributed openly in protected form but can only be viewed or used within a system that processes the required restrictions and protects the data. The proposed scheme satisfies the requirement of imperceptibility and robustness for a feasible watermarking scheme. The proposed system provides high correlation value for different cropping ratios of few videos. Also the work can be extended and implemented in real time hardware by incorporating the whole procedure in programmable logic devices like FPGA, SPARTAN or

OMAP (Open Multimedia Application Programming) processors which are also used for video processing applications. They could then be used as an integral and a vital mean that can proffer the need for a better scheme of making a secure video.

ACKNOWLEDGEMENTS

The authors would like to thank the scholars who helped them in implementing a part of the proposed work and the Institution for supporting them in pursuing research.

REFERENCES

[1]. Gaurav Bhatnagar, Balasubramanian Raman and K. Swaminathan (2008), 'DWT-SVD based Dual Watermarking Scheme', IEEE International Conference on the Applications of Digital Information and Web Technologies, pp. 526-531.
[2]. Cox, M. L. Miller, and J. A. Bloom (2002), 'Digital Watermarking'. San Francisco, CA: Morgan Kaufmann.
[3]. Ching. Y. Lin, M.Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, (2001),'Rotation, scale, and translation resilient watermarking for images' ,IEEE Trans. Image Process, vol. 10, no. 5, pp. 767–782.
[4]. Kingsbury .K (1999), 'Image processing with complex wavelets'. Philos. Trans. Math., Phys., Eng. Sci., vol. 357, p. 2543.
[5]. Kingsbury .K (1998), 'The dual-tree complex wavelet transform: A new technique for shift invariance and directional filters', IEEE DSP workshop, Bryce Canyon, UT, Paper no.86.
[6]. Lino E. Coria, Mark R. Pickering, Panos Nasiopoulos and Rabab Kreidieh Ward (2008), 'A Video Watermarking Scheme Based on the Dual-Tree Complex Wavelet Transform', IEEE transactions on information forensics and security, vol. 3, no. 3, pp. 466-474.
[7]. Liu. R and Tan.T (2002), 'An SVD-Based Watermarking Scheme for Protecting Rightful Ownership', IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128.
[8]. O'Ruanaidh J.J.K and Pun.T (1997), 'Rotation, scale and translation invariant digital image watermarking', Proc. Int. Conf. Image Processing, pp. 536–539.
[9]. Serdean C.V, Ambrose M.A and Tomlinson (2003),'DWT based high capacity blind video watermarking invariant to geometrical attacks', Proc. Inst. Elect. Eng., Vis., Image Signal Process, pp.51-58.
[10]. Schneck. P. B (1999), 'Persistent access control to prevent piracy of digital Information', Proc. IEEE, vol. 87, no. 7, pp. 1239–1249.
[11]. Pareek. N.K., Patidar. V, Sud. K.K., (2006) 'Image encryption using chaotic logistic map', Image and Vision Computing, Vol. 24, No. 9, pp. 926–934.
[12]. Shubo Liu, Jing Sun, Zhengquan Xu, Jin Liu,(2008) 'Analysis on an Image Encryption Algorithm' , International Workshop on Education Technology and Training & 2008 International Workshop on Geoscience and Remote Sensing, pp. 803- 806.
[13]. Xiao-jun Tong, Ming-gen Cui, (2007) 'A New Chaos Encryption Algorithm Based on Parameter Randomly Changing', IFIP International Conference on Network and Parallel Computing 303-307.

Thaiyalnayaki K. is a Ph.D scholar in Electronics and Communication Engineering at Anna University. She received her Bachelor degree in Electronics and Communication Engineering in 1996 at Madurai Kamaraj University. She received Master Degree in Applied Electronics from Anna University in the year 2005. Her research interests include Pattern recognition, Video encryption and signal processing.

Dhanalakshmi R. received her Bachelor degree in Computer Science and Engineering in 2001 at Madras University. She received Master Degree in Computer Science and Engineering from Anna University in the year 2010. Her research interests include Watermark and encryption and Video analysis.