A New And Secure Video Watermarking Method Based On ECC With HWD And NMF

R.V.Raviteja [1], K. Vijaya Kumar [2], K. Venu Gopal [3]
1 M.Tech. Student, St.Ann's College of Engg. & Technology, Chirala.
2,3 Asst. Prof., St.Ann's College of Engg. & Technology, Chirala.

Abstract:

Rapid growth in sharing information using Internet technologies laid the threats of copyright protection for digital multimedia contents. Watermarking and Cryptography are the balancing appearances for protecting multimedia contents. In this paper, we propose a novel approach for embedding the watermark in to the video sequences. The watermark is encrypted with Elliptical Curve Cryptography. The ECC with generator g provides better security and more efficient performance with shorter key size. Here, a new family of perfect reconstruction, non- redundant and multiresolution geometrical transform and modified versions of directional filter banks are used to decompose the video in to frequency bands. The lower frequency band is factored using Non- Negative Matrix Factorization for dimension reduction. Experimental results show that the proposed method provides a high resilience against geometrical distortions and collusion attacks.

Keywords: **Video Watermarking, Elliptical curve cryptosystem, Hybrid wavelets and directional filter banks, Non – negative matrix factorization.**

1. INTRODUCTION

The growth of the digital multimedia technology and the successful development of the internet have not only allowed to people to process, deliver and store digital content more easily, but also have gifted the facility of copyright it rapidly without loss of quality , with no limitation on the number of copies, tampering with and redistributing illegally without authorization. This kind of advantages raises the issue of how to protect the copyright ownership.

Cryptography and Watermarking are most popular multimedia security methods. In recent years, lot of efforts have been made to identify the copyright violators and protect them using cryptography and watermarking. Watermarking is an effective method and robust as compared with cryptography which doesn't provide permanent protection for the digital multimedia content after delivery to consumers.

Video contents can be mentioned as the most valuable digital media, which are increasingly used illegally resulting in a huge damage to filmmaking industry. Video Watermarking is utilized for different video applications. *Copyright protection* is the first targeting application of digital watermarking. *Copy control* is the other video watermarking application. By the demand of copyright owners and Hollywood studios, the Copy Protection Technical Working Group(CPTWG) defined a system for future DVD devices in order to prevent illegal copying of DVD disks. One of the six components of this system obligates complaint devices to check for a copy authorization watermark in the MPEG-4 video streams before playing and /or recording digital video sequences on DVDs. As another video watermarking application, *Fingerprinting* enables digital media producers to trace back the traitor customers whom have distributed copyright media with no permission through some peer-to-peer systems (e.g. ShareAza,

KazaA, eDonkey) by inserting an indelible and invisible watermark identifying the corresponding customer. This also can be done Pay-per-View (PPV) and Video- On – Demand(VOD) services by inserting the customers ID into the delivered video data. Other applications exist for video watermarking such as *Broadcast Monitoring, Video Authentication and Enhanced vide o coding*, as the most popular ones.

In Wavelet – based Contourlet Transform (WBCT), where DFB is applied to all the detail subbands of wavelets in a similar way that one constructs contourlets. The main difference is that we used wavelets instead of the laplacian pyramids employed in contourlets. The main disadvantage of WBCT is the occurrence of artifacts that are caused by setting some transform coefficients to zero for non linear approximation.

In this paper, we propose a new and secure video watermarking method based on elliptical curve cryptosystem with HWD and Non – negative matrix factorization, which is robust against collusion attack. In section2, we present a brief overview on elliptical curve cryptosystem; section3 discusses the concept of hybrid wavelets and directional filter banks. Section4 discusses the non-negative matrix factorization. The proposed embedding and detection algorithms are described in section5. The experimental results are described in section6 and finally section7 concludes the paper.

2. ELLIPTICAL CURVE CRYPTOSYSTEM

The most of the hardware and software products and standards that use public key technique for encryption, decryption are based on RSA cryptosystem. The increment in the key length can increase the security of the RSA cryptosystem, but on the other hand it requires extra computational cost. In the recent year, a new public key cryptosystem has shown his competency to challenge RSA. This cryptosystem is Elliptical curve cryptosystem. The main attraction of ECC is that it can provide better performance and security for a smaller key size, in comparison of RSA cryptosystem. In this way we can reduce computational cost. The mathematics of ECC is more complex than RSA cryptosystem.

Elliptical curves are of the form

$$y2 = x3 + ax2 + bx + c - - - (1)$$

If we have two points on an elliptical curves and draw a line through both of them, the line will intersect the curve on third point.

The following form is sufficient

$$y2 = x3 + ax + b - - - (2)$$

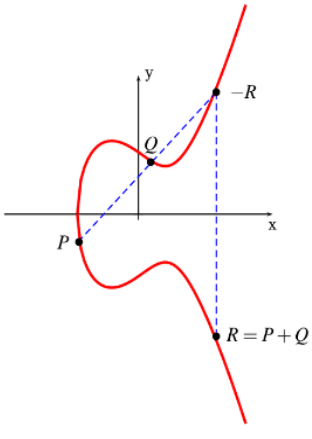


Fig1: Points on Elliptical curve

3. HYBRID WAVELETS AND DIRECTIONAL FILTER BANKS

Directional filter banks (DFB) decompose the frequency space into wedge-shaped partitions

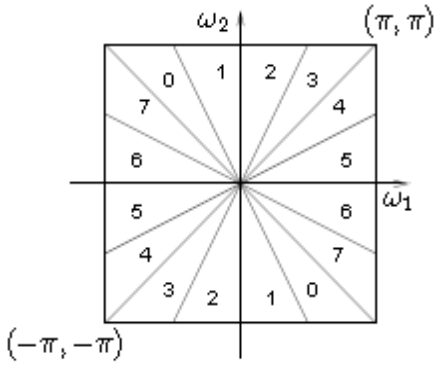


Fig2: Directional filter bank frequency partitioning using 8 directions

in figure2. In this example, eight directions are used, where directional subbands of 1, 2, 3 and 4 represents horizontal directions (directions between -45° and +45°) and the rest stand for

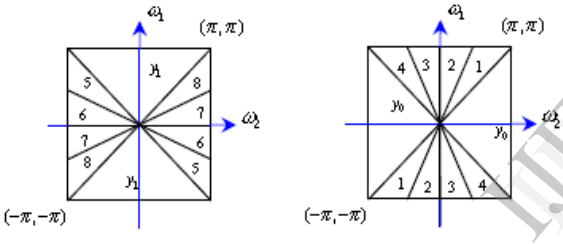


Fig 3: (a). An example of the vertical directional filter banks

(b). An example of the horizontal directional filter banks

the vertical directions (directions between (45° and 135°). The DFB is realized using an iterated quincunx filter banks. For the HWD, we required to decompose the input into either horizontal directions (or) vertical directions (or) both.

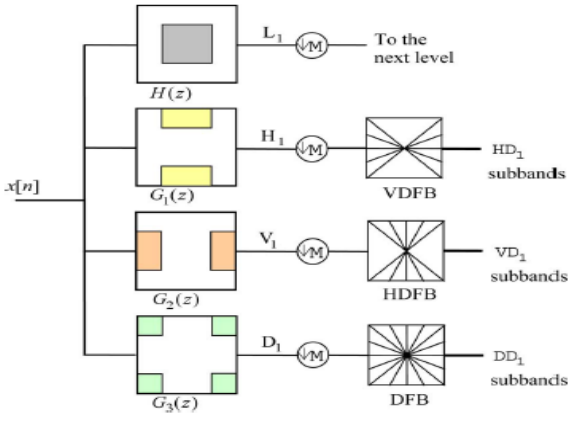


Fig 4: Schematic Plot of the HWD-H transform using 3 directional levels

For HWD, similar to WBCT, the wavelet transform as the multiresolution subband decomposition. Wavelets have shown their good nonlinear approximation property for piecewise smooth signals. By adding the feature of directionality we could improve the nonlinear approximation results from wavelets.

To reduce the artifacts in WBCT, we propose the following two types HWD family basis functions.

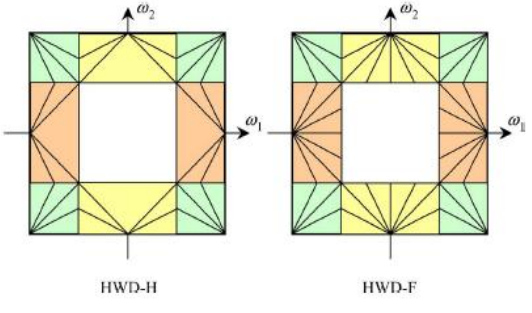


Fig 5: Frequency partitioning in the HWD using 3 directional levels

1. HWD type1

a. Apply the DFB to the m_α finest diagonal wavelet sub bands (HH_i, $(1 \le i \le m_\alpha)$

b. Apply the VDFB to the m_α finest diagonal wavelet subbands (HL_i, $(1 \le i \le m_\alpha)$

c. Apply the HDFB to the m_α finest diagonal wavelet subbands (HL_i, $(1 \le i \le m_\alpha)$

2. HWD type2

a. Apply the DFB to the m_α finest diagonal wavelet sub bands (HH_i, $(1 \le i \le m_\alpha)$

b. Apply the VDFB to the m_α finest diagonal wavelet subbands (HL_i, $(1 \le i \le m_\alpha)$

c. Apply the HDFB to the m_α finest diagonal wavelet subbands (HL_i, $(1 \le i \le m_\alpha)$

In HWD1, we further decompose the vertical and horizontal coefficients already obtained through wavelet filtering. We use the proposed modified versions of the DFB to lower the complexity and to further reduce the artifacts. In HWD2, however, we decompose the horizontal subbands vertically and the vertical subbands horizontally.

4. NON NEGATIVE MATRIX FACTORIZATION:

One major drawback of SVD is that the basis vectors have both negative and positive components, and the data are represented as linear combinations of these vectors with positive and negative coefficients. In many applications, the negative components contradict physical realities. To address this problem, the NMF approach was proposed to search for a representative basis with only nonnegative vectors.

Given a cover image C of size m × m, we can approximately factorize C into the product of two nonnegative matrices B and H with sizes m × r and r × m respectively, that is the C = BH; where r ≤ m. The nonnegative matrix B contains the NMF basis vectors, and the Nonnegative weight matrix H contains the associated coefficients. To measure the quality of the approximation factorization C = BH, a cost function between C and BH needs to be optimized subject to non-negativity constraints on B and H. This is done by minimizing the I – information divergence which is given by

$$I(C \parallel BH) = \sum_{ij} (C_{ij} \ log \frac{C_{ij}}{(BH)_{ij}} - C_{ij} \ + ((BH)_{ij}) - \quad -(3)$$

This yields the following multiplicative update results

$$\boldsymbol{H_{kj}} \leftarrow \boldsymbol{H_{kj}} \frac{\sum_i \frac{\boldsymbol{B_{ik}}\boldsymbol{C_{ij}}}{\boldsymbol{(BH)_{ij}}}}{\sum_i \boldsymbol{B_{ik}}} - - - (4)$$

$$\boldsymbol{B_{ik}} \leftarrow \boldsymbol{B_{ik}} \frac{\sum_i \frac{\boldsymbol{H_{kj}}\boldsymbol{C_{ij}}}{\boldsymbol{(BH)_{ij}}}}{\sum_i \boldsymbol{H_{kj}}} - - - (5)$$

5. EMBEDDING AND EXTRACTION ALGORITHM

The embedding and extracting procedure as follows:

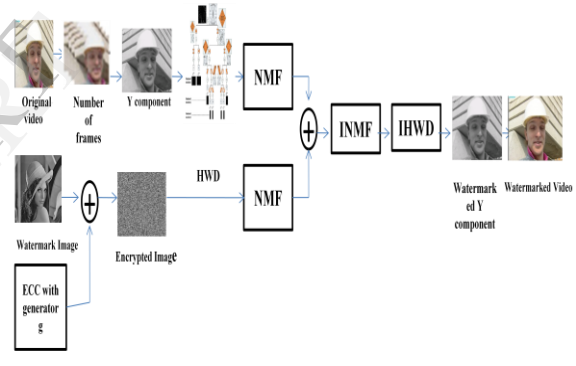


Fig 5: Embedding Procedure

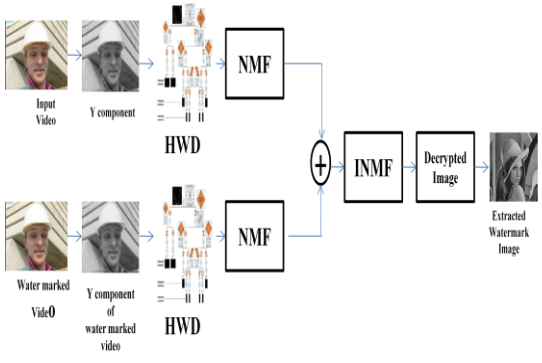


Fig 6: Extraction Procedure

WATERMARK EMBEDDING ALGORITHM:

1. Split the Video Sequence into group of frames.

2. Convert N×M RGB frames to YUV.
3. Compute the frequency domain of the luminance layer (Y) for each frame.
4. Apply HWD to frame for identifying low frequency part.
5. Input low frequency part is factorized into W_1 & H_1 by Non – negative matrix factorization (NMF).
6. The watermark image is encrypted with Elliptical Curve Cryptosystem with generator g.

   The Procedure for encrypting as follows:

   a). Encode the image as $P_{sw} = (X, Y) = (g^5, g^3)$ and similarly other points are calculated using equation

   $$y^2 + xy = x^3 + ax^2 + b$$

   b). Choose a random number k and produce the cipher text $C_{sw} = K^1G.P_{sw} + [K^1P]$
7. The encrypted image is factorized using NMF into W_2 & H_2
8. The W_1 is normalized in between 0 and 1 is termed as M_1, i.e.

   $$\boldsymbol{M_1[i] = (W_1\,[i] - \max(W_1))/\min(W_1) - \max(W_1)}$$
9. The weight matrix is obtained by

   $$\boldsymbol{Alpha = 0.05 * M1[i]}$$
10. The embedding is performed as,

    $$\boldsymbol{W_{new} = W_1 + Alpha \otimes W_2}$$

    $\otimes$ … indicates element wise product.
11. After getting W_{new}, using H_1 the INMF results the watermarked coefficients of Y component.
12. Inverse HWD is applied to get back watermarked Y component and these will combined with other channels of original video to get the watermarked video.

WATERMARK EXTRACTION ALGORITHM:

1. Split the Original and watermarked video sequences in to group of frames.
2. Convert N×M RGB frames to YUV.
3. Compute the frequency domain of the luminance layer (Y) for each frame.
4. Apply HWD to frame for identifying low frequency part in both the frames.
5. Low frequency components are factorized into W_1 and H_1 and W_m and H_m by Non negative matrix factorization.
6. The watermark is normalized in between 0 and 1 is termed as $M_{wmkd.}$

   $$\boldsymbol{M_w[i] = (W_w\,[i] - \max(W_w)) / \min(W_w) - \max(W_w)}$$
7. The weight matrix is obtained by

   $$\boldsymbol{Alpha = 0.05 * Mw[i]}$$
8. The embedding Performed as

   $$\boldsymbol{W_{new} = (W_w - W_1) \otimes Alpha}$$

   $\otimes$ … indicates element wise product.
9. After getting W_{new}, using H_2 the INMF results the extracted image.
10. The extracted image is decrypted by ECC.

    The decryption procedure as follows:

    a). To decrypt the encoded image, compute

    $P_{sw} + K^1P - n_B1K^1G = P_{sw} - K(n_B1G) + KP = P_{sw} - K^1n_B + K^1n_B = P_{sw}$
11. The extracted image is processed for NCC test.

To check the robustness of the technique, the watermarked video is processed for various attacks and then extracting part is carried out.

6. EXPERIMENTAL RESULTS

Our watermarking algorithm has been tested over different videos. We consider eight test sequences “Akiyo”, “Mother & Daughter”, “Coastguard”, “Container”, “Foreman”, “Tennis”, “Mobile” and “News” in CIF format (352×288 pixels) of 150 frames each are used in this experiment.

First we wanted to test the perceptual quality of the watermarked videos. To compare the watermarked

video with the original one, we computed the Mean Peak Signal To Noise Ratio (PSNR) of all frames of the video.

$$PSNR\ (video) = \frac{\sum_{I=1}^{F} PSNR(i)}{F} - - - (6)$$

$$PSNR = 10^{*} log_{10}\left(\frac{255^2}{MSE}\right) - - - (7)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[\,I(i,j) - K(i,j)][\,I(i,j) - K(i,j)]^2$$

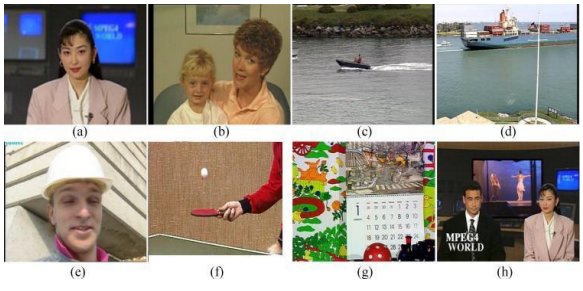


Fig 7: Test videos (a). Akiyo, (b). Mother & daughter, (c). Coastguard, (d). Container, (e). Foreman, (f). Tennis, (g). Mobile, (h). News

Fig 8: Two different original watermarks for proposed algorithm (Cameraman & pout)

The visible quality of extracted watermark and original watermark is evaluated using Normalized Cross Correlation (NCC) as,

$$NCC = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} g(i,j) \times f(i,j)}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} g(i,j)^2} - - - (7)$$

Several experiments have been carried out to evaluate the robustness of the proposed watermarking algorithm. For this purpose, some video sequence manipulations such as adding Gaussian noise, frame dropping, frame swapping and MPEG -2 compression are used.

Because the digital video data has high temporal redundancy, the frame dropping or frame cutting, which removes some frames of the video sequence, is an effective video watermark attack because it doesn't damage the video signal but the embedded watermark can be eliminated. Frame dropping attack is given by,

$$V_{attacked} = V_{original} - \{Fr1, Fr2, \ldots, Frn\} - - (8)$$

Where $V_{attacked}$, $V_{original}$ are the attacked and original video signals, and are some video frames.

A collusion attack occurs when collections of the video frames are analyzed and combined to destroy the watermark signal without distorting the video sequence to produce copies without watermark signal.

An example of such attack is the frame averaging, in which the average of the actual frame with the nearest neighbor frames is computed and used to replace the actual frame as given as,

$$F_r{}^{1}{}_{(i,j)} = \frac{1}{3}\left[F_{r-1\,(i,j)} + F_{r\,(i,j)} + F_{r+1\,(i,j)}\right] - - - (9)$$

Frame swapping attack, on the other hand, can destroy some dynamic composition of the video signal and also the embedded watermark. This attack is formulated as

$$F_r(i,j) \Leftrightarrow F_{r+1}(i,j), r = 1,3,5,\ldots R-1 - - - (10)$$

The other attacks were JPEG compression, resizing, adding Gaussian noise, Low pass filtering, rotation, histogram equalization, contrast adjustment, gamma correction, cropping, rewatermarking. Matlab 7.0 (R12) was used to test all attacks.

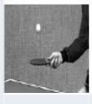
Type of the Attack	Original Video	Watermarked Video	Encrypted Image	Extracted Watermark	PSNR (dB)	NCC
1. No Attack					42.43	1.00
2. Gaussain Noise (μ = 0, Var = 0.001)					41.23	1.00
3. Contrast Adjustment([l=0,h=0.8],[b=0, t=1])					41.89	0.8655
4. JPEG compression (Q=25)					33.973	0.8434

Table1: Original and Watermarked videos with different attacks with PSNR and NCC values of Tennis Video sequence

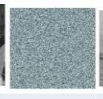
Type of the Attack	Original Video	Watermarked Video	Encrypted Image	Extracted Watermark	PSNR (dB)	NCC
9. Collusion (cameraman with pout image)					35.622	0.989
10.Resising(256 512)					36.456	0.5476
11. Gamma Correction (Gamma=0.9)					39.65	0.8095
12. Frame Swapping (First six frames)					32.804	0.9523

Table3: Original and Watermarked videos with different attacks with PSNR and NCC values of Tennis Video sequence

Type of the Attack	Original Video	Watermarked Video	Encrypted Image	Extracted Watermark	PSNR (dB)	NCC
5. Cropping (both sides)					19.285	0.905
6. Sharpening					21.147	0.966
7. Histogram Equalization					31.600	0.8500
8. Rewatermarking					33.973	0.8434

Table2: Original and Watermarked videos with different attacks with PSNR and NCC values of Tennis Video sequence

Type of the Attack	Original Video	Watermarked Video	Encrypted Image	Extracted Watermark	PSNR (dB)	NCC
13. Frame Averaging (Average first 3 frames)					32.957	0.836
14. Frame Insertion (Fifteen frames Inserted)					34.1123	0.911
15. Salt & pepper noise(0.02)					33.839	0.6061
16. Rotation & scale (5 degree & 0.5)					31.6002	0.8566

Table4: Original and Watermarked videos with different attacks with PSNR and NCC values of Tennis Video sequence

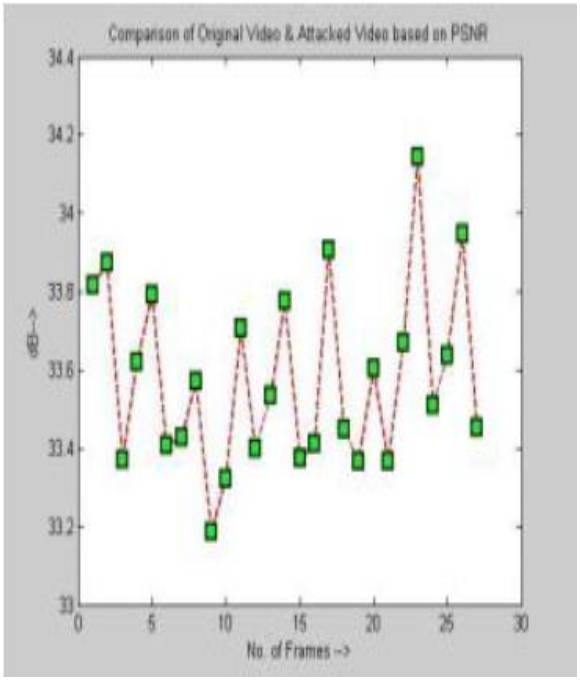


Fig: PSNR values with different attacks for tennis video sequence.

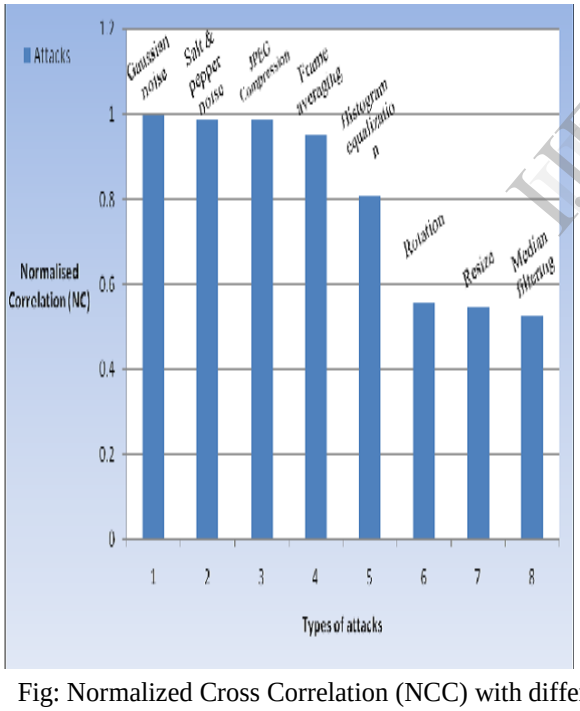
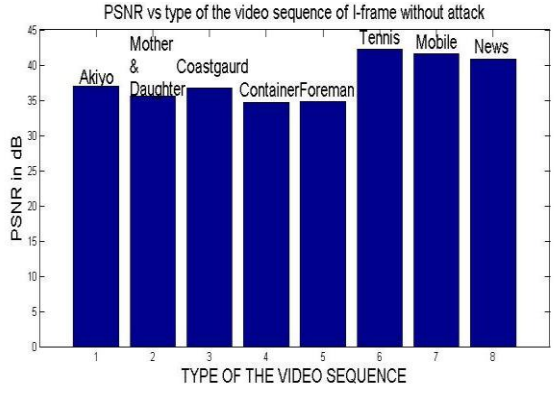


Fig: Normalized Cross Correlation (NCC) with different attacks



7. REFERENCES

[1]. Petticolas.F,Stefan.k, " Information hiding techniques for steganography and digital watermarking", ISBN 158053-035-4, December 1999.

[2]. Hartung F, Kutter M, "Multimedia watermarking techniques", IEEE transcations on image processing, 1999.

[3]. G. Doerr and J. Dugelay, "A guide tour of video watermarking", signal processing: Image communications, ELSEVIER science, vol 18, 2003, pp.263-282.

[4]. J. Bloom, I. Cox, T. Talker, J.P. Linnartz, M. Miller, C.Traw, "Copy protection of DVD video", Proceedings of the IEEE, vol. 87(7), 1999, pp.1267-1276.

[5]. P.W. Chan, M.R.Lyu, R.T. Chin, "A novel scheme for hybrid digital video watermarking", IEEE transactions on circuits and systems for video technology, vol.15, no.12, December, 2005.

[6]. Ramin Eslami, Hayder Radha," A new family of nonredundant transforms using Hybrid wavelets and directional filterbanks", IEEE transactions on Image processing, vol.16, no.4, April 2007.

[7]. Ramin Eslami, Hayder Radha, "Image watermarking using hybrid wavelets and directional filterbanks", IEEE transactions on Image processing, June,2006.

[8]. D. Lee and H. Seung, "Algorithms for nonnegative matrix factorization", Adv. In neural info.proc. systems, 13, 2000.

[9]. "The case of Elliptical Curve Cryptography", National security Agency, 2009.

[10]. Vinod kumar yadav, Dr. A.K. Malviya, D.L.Gupta, Satyendra singh, ganesh Chandra, "Public key cryptosystem technique Elliptical Curve Cryptography with generator g for image encryption, IJCTA, vol.3(1), Feb. 2012.

[11]. Th. Rupachandra Singh, Kh. Manglem singh, Sudipta Roy, " Video watermarking scheme based on visual cryptography and scene change detection", ELSEVIER, 2013, pp.645-651.

[12]. Salwa A.K., Mostafa, A.S. Tolba, F.M. Abdelkadar, Hisham M. Elhindy, " Video watermarking scheme based on principal component analysis and wavelet transform, IJCSNS, Volume 9, no.8, August 2009.

R.V.Raviteja is presently pursuing M.Tech.Degree from St.Ann's College of Engineering & Technology, Chirala. Presently, His current research interest includes Digital Video Watermarking, Scalable video coding.

Kurapati. Vijaya Kumar received M.Tech. Degree from Bapatla Engineering College, Bapatla in 2008. Presently, he is working as an Asst. Prof. in the Dept. of ECE of St. Ann's College of Engineering & Technology, Chirala. He is having 6 years of teaching experience. His current research interest includes Digital Video Watermarking, Signal Processing in Encrypted domain and High Efficiency Video Coding (HEVC).

K. Venu Gopal received M.Tech. Degree from SRM University, Chennai in 2007. Presently, he is working as an Asst. Prof. in the Dept. of ECE of St. Ann's College of Engineering & Technology, Chirala. He is having of 7 years of teaching & Industrial Experience. His current research interest includes Digital Video Watermarking, Embedded Systems.