*International Journal of Latest Engineering and Management Research (IJLEMR)*
*ISSN: 2455-4847*
*www.ijlemr.com || Volume 02 - Issue 11 || November 2017 || PP. 32-38*

# Watermarking scheme for the security of critical multimedia data

Fariya Faizel,
*(Toch Institute of Science and Technology, India)*

**Abstract:** Pace at which the technology evolves astonishes the world. As the technology grows, more and more data is created and there is a high need to secure these data. The copyright protection and the authentication of the data is a critical issue to be attended .This paper proposes a method for copyright protection and authentication of multimedia data such as digital images and digital videos. This scheme uses image processing transforms, single value decomposition and compressing sensing measurements to achieve security of the multimedia data .In this scheme host medium is digital image or video and the generated watermark data have many different security layers from embedding factor, measurement matrix. The orthogonal matrices, wavelt basis matrix also provides security. This scheme offers protection against various standard watermarking attacks such as signal processing attacks, compression attacks and the geometric attacks. This scheme provides high payload capacity. This scheme performs efficiently and faster than the existing systems.

**Keywords:** Compressive sensing measurements, Curvelet, Multimedia, Video, Watermarking

## 1. INTRODUCTION

Digital images, digital videos, and texts are transferred through the cloud, mobile and internet. Multimedia data are copied and transferred by the imposter without the copyright and the imposter use this data at many different places by the use of internet, mobile and cloud access. This is an issue of copyright protection and authentication. Watermarking is the solution for copyright authentication and protection of multimedia data.

Watermarking is of two types robust watermarking and fragile watermarking [1]. The robust type watermarking gives robustness against the manipulation or attack. Robustness in watermarking means the watermark data can be extracted from the watermarked data even when the watermarked data is corrupted or modified. It is used for copyright protection of multimedia data. Fragile type watermarking gives fragility against the attacks and manipulation. Fragility in watermarking means watermark data cannot be extracted when watermarked data is corrupted or modified. This type of watermarking technique is used for copyright protection and authentication of multimedia data. Design of watermarking technique can be of various domains such as spatial, transform, hybrid and sparse [2] The spatial technique is less robust. Transform technique is preferred for the security of multimedia data than the spatial as it is more robust. It has limited payload capacity. The hybrid technique has more than two images transform and provides more impercetability. Sparse technique is the new technique which utilizes compressive measurements. It provides better payload and authenticity. Various schemes for watermarking are pre sented by researchers for the security of multimedia data. Spatial techniques are proposed using LSB substitution, correlation properties of different noise sequences for digital videos and images for the security of multimedia data[2,34,5]. These techniques have limitations such as it is less robust against various attacks. T ransform n techniques were proposed to overcomes the limitation of spatial domain techniques [6]. In this technique, image transforms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are used for watermark embedding [7]. This techniques have more robustness and less payload capacity than the spatial techniques. This technique is used for copyright protection of multimedia data. Hybrid techniques by various utilizes two or more than two image transformations such as DCT + DWT, DWT + SVD, DCT + DWT + SVD are used for watermark embedding[8]. It has more robustness and imperceptibility. Its limitation is less payload capacity. Donoho and Candes introduced a signal acquisition theory named as CS theory [9]. Watermarking technique based on CS theory is known as sparse techniques.In this sparse information of watermark is used. The robust CS theory based techniques are for themultimedia data protection [10].

Most watermarking techniques are used for the copyright protection of multimedia data and only few watermarking techniques are designed and used for copyright authentication of multimedia data.Payload capacity of existing watermarking techniques are less. Therefore hybrid CS theory based watermarking scheme is proposed for authentication of multimedia data which provides high payload capacity. Transform techniques, hybrid techniques and sparse techniques have many drawbacks so a hybrid watermarking scheme using DCT, DWT, SVD, and Curvelet transform with a combination of CS theory is proposed in this paper. In this scheme, the CS theory is applied on watermark image to generate CS measurements. The discrete wavelet transform (DWT) and singular value decomposition (SVD) is used for CS measurements. The high

frequency curvelet coefficients of Discrete cosine transform coefficients of host image are modified according to sparse data of watermark image to generate watermarked image. CS theory is used in this scheme because it provides an additional layer of security. This scheme has good execution time and authentication of multimedia data.

## 2. PRELIMINARIES

### 2.1. Discrete cosine transform

It represents an image as a sum of sinusoids of varying magnitudes and frequencies. In Dct, most of the visually significant information about the image lies in just a few coefficients. Discrete cosine transform is used to convert the image into transform domain. Transform domain is a mathematical procedure done on data. It is used to convert it from one domain to another that is from time to frequency.In this new domain the data is easily handled, transformed back to its originl data. The transformed matrix consists of both ac and dc coefficients. If the Dct is applied on block size N×N,then it is called block Dct .In Dct transformed block the left top corner element is called a dc coefficients which is perpetually significant while other are ac coefficients which are less significant. These coefficients are zig zag scanned to obtain frequency components of an image in decreasing order.

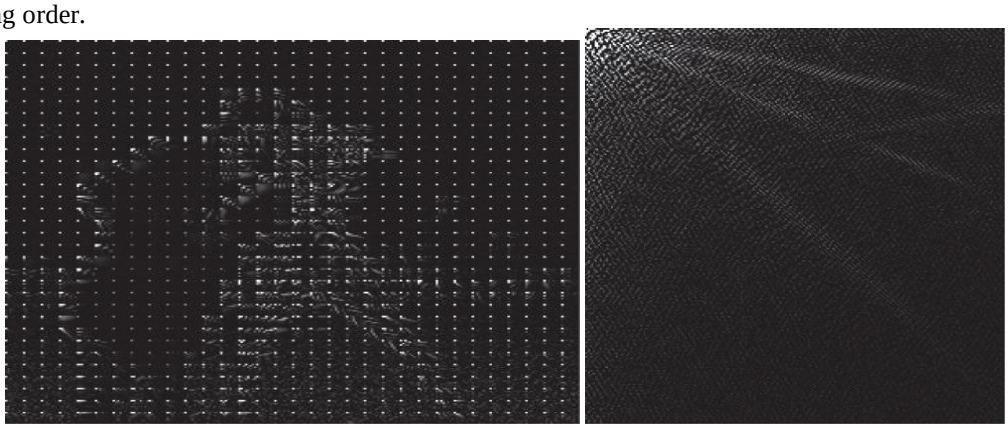


Fig1: dct coefficients of image

### 2.2. Discrete curvelet transform

It decomposes the image into various frequency cells. Its divided into low frequency cell and high frequency cell. It represents image into its sparse domain. There are two discrete transforms are available such as frequency wrapped based and unequally spaced fast fourier transform technique based. Frequency wrapping based discrete curvelet transform have less execution time and easy to implement compared to other curvelet transforms.

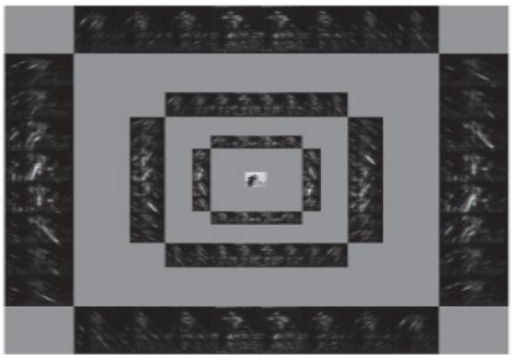


Fig 2: All curvelet coefficients

### 2.3. Discrete wavelet transform

It decomposes the image into various frequency coefficients .These coefficients are different than other coefficients. It plays an important role in image processing applications, image compression, compressive sensing and watermarking. Discrete wavelet transform decomposes image in various frequency subbands such as approximation, horizontal, vertical, diagonal. The visual information of the image is laid on approximation wavelet subband. These subbands have low frequency coefficients. Horiontal, vertical and diagonal have high frequency coefficients. There all wavelet subbands gives sparsity property. When the wavelet basis matrix with

its inverse version is applied on image then the image is converted into its wavelets.Wavelet matrix is generated using wavelet matrix generation.The various orthogonal wavelets such as haar,bior6.8,and symlet are used for wavelet matrix generation.

**2.4. Single value decomposition**

It's a linear algebra tool which decomposes the image into singular value matrix and two orthogonal matrix. Singular value matrix has non negative values diagonally placed in the matrix. It has sparsity and stable property which is suitable for spaces coefficient generation in compressive sensing. It is used for generation of sparse coefficient.

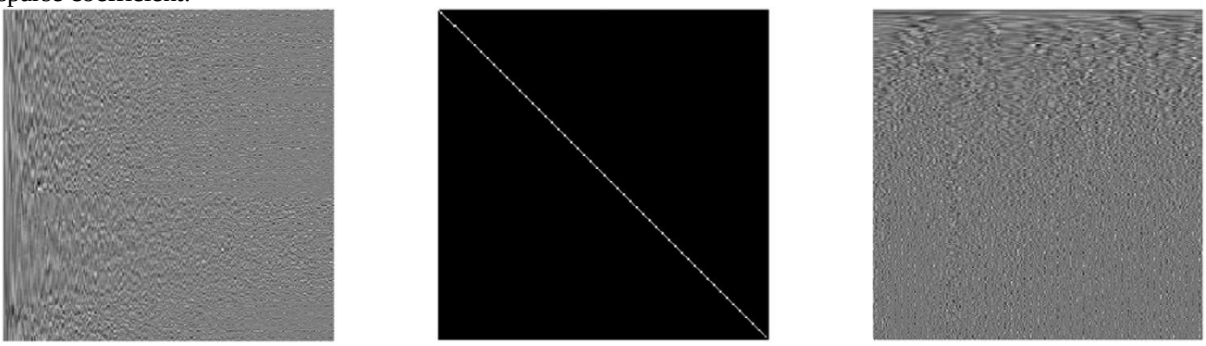


Fig 3: SVD Matrices of Image

**2.5. Compressive sensing**

It is a signal processing technique for effectively capturing and reconstructing a signal by finding solution to underdetermined linear system. Underdetermined system of linear equation has more unknown and generally has infinite number of solution. There are two conditions under which the recovery is possible. First one is sparsity which requires the signal to be sparse in some domain. The second one is incoherence which is applied through the isometric property The CS measurments based watermarking technique is used to identify tamper of an image using standard logo or image. It embedds CS measurements of the watermark into host image by the size of CS measurements is less than the size of the host image. The hybrid watermarking techniques have less payload capacity for the large watermark data embedding. The watermarking scheme should have fast computational time, more payload capacity and authenticity.

## 3. PROPOSED SYSTEM

**3.1. Watermarking Embedding Procedure**

The watermark image is transformed into sparse domain orthogonal basis matrix. The CS measurements of watermark image which generates compressive sensing (CS) with measurement matrix. y of watermark image is embedded into the high frequency coefficients of DCT of the host image, which is used to provide a different level of security. Wavelet basis matrix is applied with its inverse and is multiplied with the w to get the wavelet coefficients. Single value decomposition is applied on the wavelet coefficients of the watermark image to obtain singular matrix and two orthogonal matrices. The sparse coefficients is chosen as singular matrix value of wavelet coefficients .Measurement matrix which is Gaussian in nature is applied on the singular value of wavelet coefficients of watermark image to obtain cs measurements.

**3.2. Watermarking Extraction Procedure**

For extraction of the watermark from watermarked image embedding factor, sampling factor, the measurement matrix, wavelet basis matrix, and orthogonal matrices U, V are required. Apply discrete cosine transform on the Watermarked image to get the modified DCT coefficients. Apply frequency wrapping based fast discrete curvelet transform on DCT coeffi- cients to get its modified curvelet coefficients values Then get modified high frequency curvelet coefficients which are used for watermark embedding. Extract sparse data of watermark image using modified high frequency curvelet coefficients and embedding factor. Apply upsampling procedure with sampling factor security key on sparse data to get CS measurements of watermark image The measurement matrix A which is used as security key 3 and recovered the singular value of watermark image with the help of OMP algorithm. Apply inverse SVD to extract wavelet coefficients of watermark image and apply inverse DWT to reconstruct watermark image.

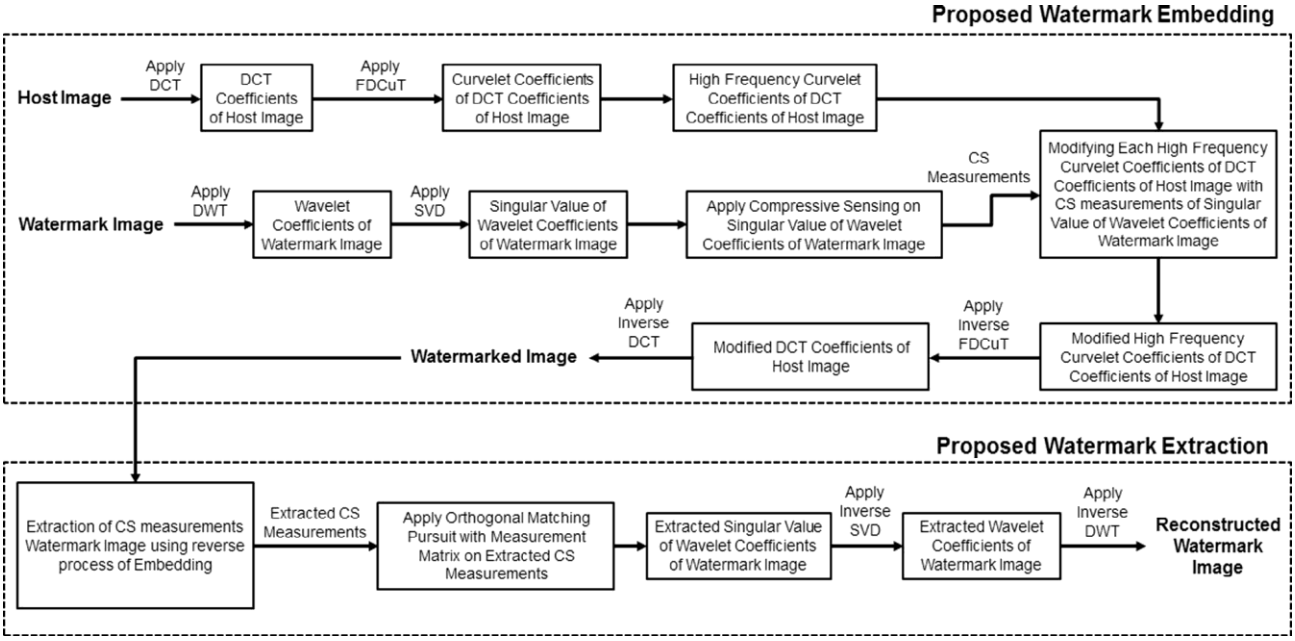
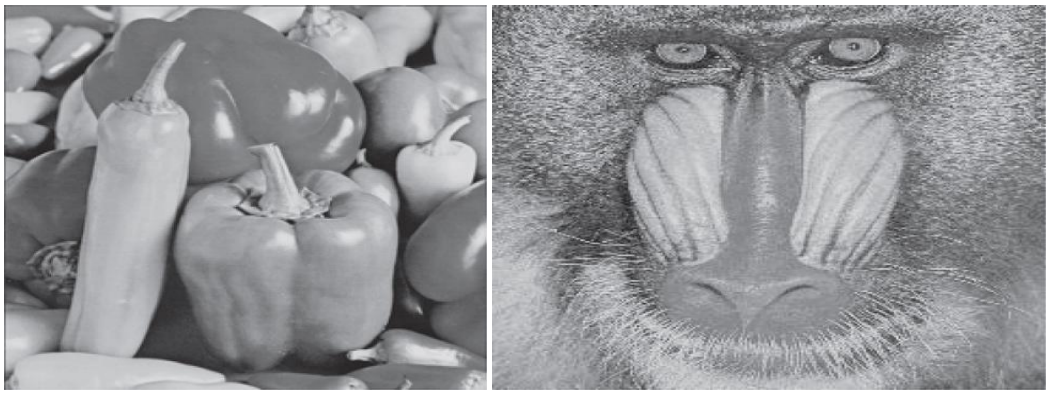



Fig 4: Proposed System

## 4. RESULT AND DISCUSSION

Testing with digital image and video with quality measure is discussed here. PSNR, SSIM are the quality measures. Effects of watermarking attacks on authentication the effect of wavelets on perpetual quality and performance, comparison with the existing system is discussed here. Performance of any watermarking scheme varies with different types of images. Two different types of host images such as cameraman image which has low frequency coefficients and lady image of high frequency coefficients are used. The JPEG compression with different quality factor, Salt and pepper noise, speckle noise, filter attacks such Median, sharpen. mean and low pass Gaussian filter ,histogram equalization, rotation and cropping. The perceptual quality of watermarked image is measurement by Peak to Noise Ratio. The MSE measurement is logarithmic scale when PSR is measured. Structure similarity index measure is used to check for the similarity between original and reconstructed watermark image. When the SSIM value is 1 it indicates that the reconstructed and watermarked images are same. If it is 0 then it signifies that it does not match. The jpeg compression is used when transmission of data happens in a medium. Different quality factor tries to reconstruct the watermark image after JPEG compression. SSIM and PSNR values is 47.19 dB, 40.51 Db ,1.00.Fig 5 explains the host images and Fig 6 shows result of this scheme without watermarking attacks. The value for camera host image and lady host image are 1.00,1.00. The sampling factor β is 0.0001 for all the watermarked image with attacks and without attack. Predefined threshold and sampling factor τ and β are chosen as per the user .Haar, Bior 6.8 and Sym8 are used here for the generation of sparse coefficients.

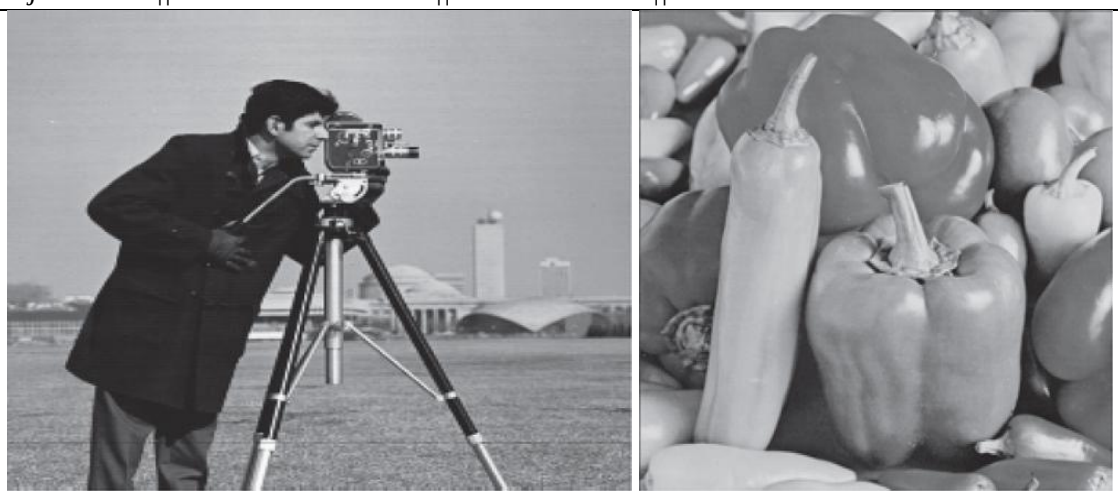
(a) (b)



( c ) (d)

Fig 5: Host images (a) cameraman (b) lady (c) peppers (d) mandrill

For the implementation of video, the digital video is broken out into various frames. Watermark image is embedded into individual video frames to generate individual watermarked frames. These watermarked frames are then combined to get watermarked video. Embedding factor and sampling factor for watermarked video frame generation is 0.02 and 0.0001. Performance analysis of proposed scheme for video is performed by taking one watermarked video frame on which watermark image is embedded. Watermarking attacks is applied on this watermarked video frame to get watermark image from corrupted or modified watermarked video frame. It is used for copyright ownership and authentication of any digital video.



(a) Watermarked Cameraman Host images (b) Reconstructed Peppers Watermark Image

(a) Watermarked lady host Image (b)Reconstructed Peppers Watermark Image

Fig 6: results of proposed scheme without watermarking attack

The execution time is divided into watermark preparation time, watermark embedding time, watermark extraction time and watermark reconstruction time. This system applies compressive measurements on watermark image before embedding while existing schemes embed watermark image directly into host medium. This system uses four image processing transforms while existing scheme uses one or two image processing transforms. The payload capacity of proposed scheme is 65 K bytes while that of existng schemes is up to 17 K bytes. The performance measures of this system is better than existing schemes available in the literature.

## 5. CONCLUSION

A hybrid watermarking technique is proposed in this paper. This scheme provides high payload capacity and have faster execution time. Execution time for watermarked data genertation and extraction of watermarked data is 3.93 sec. This scheme is used for authentication to transfer digital data over cloud and high speed internet. This scheme provides copyright authentication and ownership us in various security keys. The authentication of multimedia data is verified against from watermarking attacks like filter attacks, geometric attacks, compression attacks, noise addition attack with different embedding factor. The PSNR of wavelet packets show that its better performed when cs measurements are generated using Haar wavelet. The quality measure of the proposed system is better than the existing schemes.

## REFERENCES

[1] Langelaar .G., Setyawan. I,Lagendijk., Watermarking of digital image and video data-A state of art review. *IEEE Signal Process*.Mag 2000,20-46.

[2] Thanki R,Kothari A,Digital watermarking – Technical art of hiding a message.*Intell.Anal.Multimedia Inf*.2016,426-460.

[3] Ramalingham M,Stego machine-video steganography using modified LSB algorithm.*World Acad.Sci.Eng.Technol 74*.,2011,502-505.

[4] Koz A,Alatan A,Oblivious spatio terporal watermarking of digital video by exploiting the human visual system.*IEEE Trans Circuits Syst.Video Technol 18(3)*,2008,326-337.

[5] Chan C,Cheng L,Hiding data in images by simple LSB substitution Pattern *Recogn 37*,2004,469-474.

[6] Arena S,Caramma M,Lanchi R, Digital watermarking applied toMPEG-2 coded video sequences exploiting space and frequently masking ,*Proc.int.Conf Image Process* 2,2000,796-799.

[7] Essaouabi A,Ibnelhaj E,A 3D wavelet based method for digital video watermarking In:Proceedings of the *4th IEEE Intelligent Information Hiding and Multimedia Signal Processing*,2009.

[8] Raval M,Rege P,Discrete wavelet transform based multiple watermarking scheme.*Proc,Convergent Technol,Asia-Pacific Region 3*,2003,935-938.

[9] Donoho D ,Compressed sensing *IEEE Trans.Inf.Theory 52(4)*,2006,1289-1306.

[10] Tiesheng F ,Guiqiang L,Chunyi D,Danhua W ,A Digital image watermarking method based on theory of compressed sensing *Int.J.Autom.Control Eng2(2)*,2013,56-61