'Futurizm 14', (14th & 15th March 2014), 'Pune District Education Association's College of Engg.Manjari (BK)', 'Pune 412307',Chief Editor:'Dr.K.R.Harane',Editor: 'Prof D.O.Patil', 'Prof R.M.Sahu'.

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-8 , May, 2014

Digital Steganography by DCT & SVD Data Hiding Using Colour video

*Jayashri B. Shelar, A.P.Rao.
Department of Electronics & Telecommunication
Jaywantrao Sawant College of Engg.
Pune university,Pune, Maharashtra, India 411 028
Email: jayashri.shelar@yahoo.co , prof.a.p.rao@gmail.com

Abstract: Since all the multimedia products are released via internet so it is need to protect the data from malicious attacks. Hence, there is strong need of developing the techniques to face all these problems. Digital Watermarking emerged as a solution for protecting the multimedia data. This paper , we propose a method of transform domain watermarking based on Discrete Cosine Transform (DCT) and Singular Value Decomposition Technique. this scheme embeds the watermark into cover colour video. Signature Data is embedded in individual cover colour video frames in (Red, Green, Blue) RGB Space. The Combination of Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) OF Blue channel is used to embed the signature data .The parameter used to test the robustness of proposed algorithm are peak signal to noise ratio (PSNR), Mean Square error (MSE). The Experimental result shows that the proposed method is more robust and the watermarked image has good transparency.

Key Words: Steganography, DCT, SVD, digital watermarking, Embedding and Extracting Algorithm.

I. INTRODUCTION:

The internet and the World Wide Web have revolutionaries the way in which digital data is distributed. The widespread and easy access to multimedia content has motivated development of technologies for digital steganography or data hiding, with emphasis on access control, authentication, and copyright protection. Steganography deals with information hiding, as opposed to encryption.[1] Steganography is define as follows "Steganography is the art and science of communicating in a way which hides the existence of The communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. Much of the recent work in data hiding is about copyright protection of multimedia data. This is also referred to as digital watermarking. One of the main objectives of this watermarking is to be able to identify the rightful owners by authenticating the watermarks. As such, it is desirable that the methods of embedding and extracting digital watermarks are resistant to typical signal processing operations, such as compression, and intentional attacks to remove the watermarks. The capability to hide large amounts of data will also enable robust hiding of digital watermarks by introducing redundancies in the data.

In the literature, many schemes uses the SVD-DCT based embedding for grey scale image watermarking.[6] The proposed scheme embeds the monochrome watermark into colour cover Video. The colour image is represented by Red (R), Green (G) and Blue (B channels. Out of these three channels,) change in the intensity of R channel is the most sensitive to human eyes whereas for B channel it is least sensitive Hence, in the proposed scheme the blue channel is considered for embedding.[2] To improve the robustness of

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-8 , May, 2014

the scheme the watermark is embedded into singular values of different sub-band coefficients obtained from B channel of the colour image.

The following terminology is used in this paper. The signature or message data is the data that we would like to embedded. The source data is used to hide the signature data that is we colour video in this we use only BLUE channel for hiding the signature.[2] we often refer to the source as the host data. After embedding a signature in to a host, we get the watermarked or embedded data. The recovered data, also referred to as the reconstructed data, is the signature that is extracted from the embedded data.

There are three main requirements of DigitalWatermarking. They are:
Transparency or Fidelity: The digital watermark should not affect the quality of the original image after it is watermarked. Transparency or Fidelity is defined as "Perceptual similarity between original and watermarked versions of the cover work".
Robustness**: It** is the ability of a system to cope with errors during execution.
Capacity or Data Payload: This property describes how much data should beembedded as a watermark to successfully detect during execution.

Digital Watermarking Applications
Copyright Protection
Content Identification and Management: The speed with which digital content travels across theinternet provides new opportunities for both the contentcreators and consumers if the contents can quickly and easily are identified and managed
Communication of Ownership and Copyrights**:** Digital content continues to proliferate as today'sconsumers seek information and entertainment on theircomputers, mobile phones and some other digital devices.In our cyber culture, digital has become a primary meansof communication and expression.
Document and Image Security: In today's corporate world, images and documents travelwidely and rapidly in multiple manifestations, throughemail and across the Internet. Controlling and protecting sensitive or confidential documents and images hasbecome impossible. Corporations have very littlevisibility into exactly where their documents are being accessed or by whom. Authentication of Content and Objects (includes government IDs) :The impact of counterfeiting is significant, both in termsof lost revenue for businesses and fraud to the consumer,which can even endanger citizens in the case ofcounterfeit pharmaceuticals. It is clearly a global problem that affects numerous industries, and the problem isgrowing.

Digital watermarking, when used as part of alinked and layered security approach can provide a strongdeterrence to counterfeiting and help to solve this costlyand challenging problem. Implementation of thetechnology is relatively simple with minimal impact to most workflows.

II. PRESENT METHODS

1. SINGULAR VALUE DECOMPOSITION (SVD)

In linear algebra, the singular value decomposition (SVD) is factorization of a real or complex matrix, with several applications in signal processing [2]. The SVD can beseen as a generalization of the spectral theorem toarbitrary, not necessarily square matrices. The basic ideabehind SVD is taking high dimensional highly variableset of data points and reducing it to a lower dimensionalspace that exposes the substructure of the original data more clearly.

The Singular Value Decomposition of image I of size m X n (m obtained by the operation)

$$I = USV^T$$

Where U is column –orthogonal matrix of size m*n ,S is the diagonal matrix with positive or zero elements of size n*n orthogonal matrix V. The diagonal entire of matrix S are known as the singular values of I. The columns of U matrix are known as left singular vector and the columns of the matrix V are known as right singular Vector of I. Thus each Singular value represent the luminance of image layer and the corresponding pair of singular vector represent the geometry of the image layer .In SVD based image watermarking ,several approaches are possible .A common method is to apply svd to the entire cover image and modify all the singular values to embed the watermark. The imported property of SVD based watermarking is that the large of the modified singular values of image will change by very small values for different types of attacks.

2 Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is a orthogonal transform for digital image processing and signal processing with advantages as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT method is used to convert time domain signal into frequency domain signal. Using DCT,

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-8 , May, 2014

an image is easily split into pseudo frequency bands and in this work watermark is inserted into all those frequency bands like as low, middle and high.

A DCT is a Fourier related transform similar to Discrete Fourier Transform (DFT) but using only realnumbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since Fourier transform of real and even function is real and even)[5].

III. PROPOSED METHOD

DCT –SVD Method

Robustness, capacity and imperceptibility are thethree important requirements of an efficient watermarking scheme. SVD based watermarking scheme has high imperceptibility. Although the SVD based schemewithstands certain attacks, it is not resistant to attacks likerotation, sharpening etc. Also SVD based technique hasonly limited capacity [6]. These limitations have led to the development of a new scheme that clubs the properties of DCT and SVD. This particular algorithm proves to better than ordinary DCT based watermarking and ordinary SVD based watermarking scheme.

In this paper, we will combine DCT and SVD to develop a new hybrid colour video watermarking scheme that is resistant to variety of attacks. The proposed schem is given the following algorithm.

The Embedding algorithm of DCT-SVD is described as.

We now summarize the various steps in the embedding procedure. Fig.1 gives the details of the embedding procedure.

1) Read input colour video and Signature image.
2) Convert video in to multiple frames
3) select the input frame (A) in which, to hide the signature data (D).
4) Separate Red (Ar), Green (Ag) and Blue (Ab) channel from the selected input frame.
6) Apply pre-processing for signature image(D) and apply SVD to get the singular values of logo image. U2,S2,V2
7) Embedded the'S2' component of logo image with cover image (S1) using alpha. (Alpha = 0.01). to get modifies 'S' component (mS),
8) Apply the SVD on cA coefficient to get the singular values.U1,S1,V1
9) Apply inverse SVD (U1*mS*V1') and apply inverse DCT on
10) Apply the DCT on Ab channel input image to produce dct coefficients (cA).
11)
12) Modified coefficients to produce Stego B channel.
13) Reconstruct the Stego colour image using original R and G colour components.
14) Reconstruct into video.

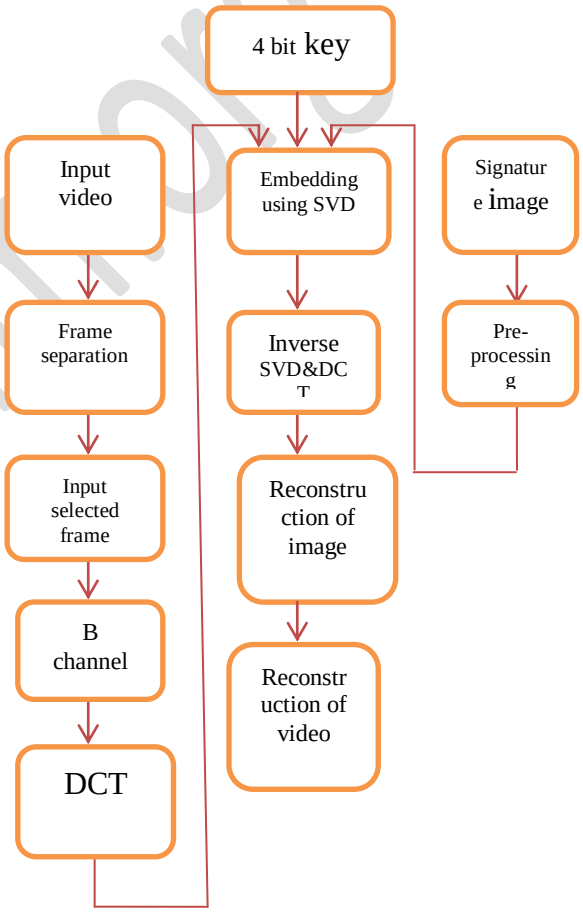

Fig.1: Embedding Process

The Extraction algorithm of DCT-SVD is described as.

We now summarize the various steps in the extraction procedure.Fig.2 Gives the details of the extraction procedure.

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-8 , May, 2014

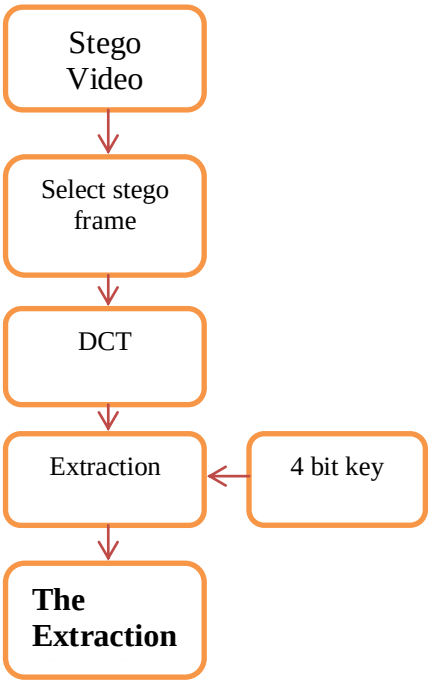

Fig.2 Extraction Process

1) Selected the stego frame and separate the R,G and B Channels.
2) Apply DCT On B channel

3). Apply Svd on Stego B channel to get singular values. U3, S3, V3
4). Extract the eS component signature image by finding the difference between S3 and S1 with alpha, by applying inverse svd for U2*eS*V2' to get Signature image.

IV. RESULTS & DISCUSSION

Peak Signal to Noise Ratio & Mean Square Error (MSE

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \Sigma_{MN} [I1(M,N) - I2(M,N)] / (M * N)$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

In the previous equation, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc

The series of experiments are conducted to analyse the effect of embedding & extraction algorithm on the input colour frame .In this paper we are hiding the signature in colour video frame using DCT,SVD & combination of DCT-SVD tech. this is our proposed method .

Table shows the comparison between only DCT & SVD methods and DCT-SVD method which is our proposed method. Higher the value of PSNR, it is hard to be aware of the difference with the cover image by human eye system. The lower the value of MSE, the lower the error.

S.no	Method	PSNR	MSE
1	SVD	23.4213	295.7686
2	DCT	22.6979	349.3741
3	DCT + SVD	42.6026	3.5713

Table-1 Values of parameters between original and extracted watermarked using DCT, SVD & DCT-SVD method Figure 3 ,4 & 5 shows the embedded & extracted images of DCT & DCT-SVD method.

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-8 , May, 2014

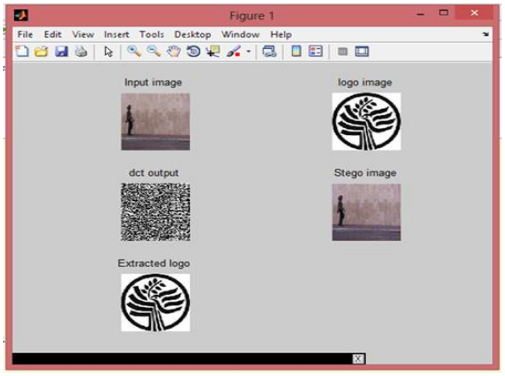

Fig.3: Embedded & Extracted image using DCT method.

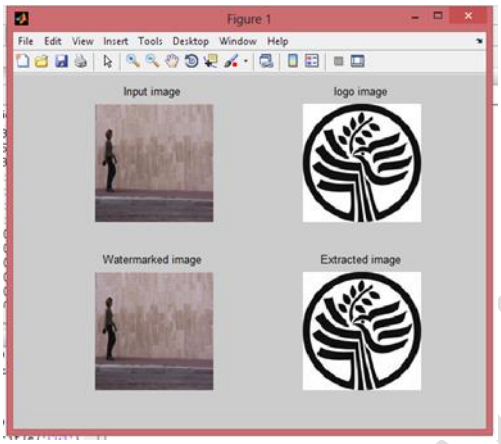

Fig. 4: Embedding & Extraction using SVD method

Fig. 3 shows the experimental result of DCT method. Fig.4 shows the experimental result of SVD method and fig.5 shows the experimental result of DCT-SVD method. Table 1 Shows the MSE & PSNR for different methods

In our proposed method we are using Hybrid of DCT-SVD technique for Embedding and Extraction process,[7] due to this hybrid combination our result is better than existing methods. We are getting high PSNR value and less MSE value. And Robustness of our system is increased due to Hybrid combination.

a. Input Image

b. logo Image

b. B-panel Image

c. DCT for B-panel

d. I DCT for Watermarked B-panel

e. watermarked Image

f. Extracted logo

Fig. 5: Embedding & Extraction using DCT-SVD method. Fig. a, b, c, d, e, f& g shows the results of each step.

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-8 , May, 2014

V.CONCLUSION:-

The Approach of the present work is based on Digital Colour Video Steganography, that further it is observe that the present technique gives better results in comparison SVD or DCT Technique. .This combination of DCT-SVD approach can be used for authentication & Data Hiding purposed. The SVD is an efficient tool for Watermarking in DCT domain. Watermark embedded using this DCT-SVD algorithm is highly imperceptible. Also extract the signature image without losses.

REFERENCES

[1]"Digital steganography (Data Hiding in Video Signal)" Priyanka Sonawane, Prof.J.S.Chitode Proceeding of the International Journal of Science & advanced Tech. ISSN 2221-8386 Volume 2 no.4 April 2012.

[2]. "No Blind watermarking scheme for colour images in RGB space using DWT-SVD" Proceeding of in 978-1-4244-9799-7/11 IEEE 2011 by Nagraj V. Dharwadkar B.B., Amberker & Avijeet Gorai. Dept. of Computer Science & Engg. Warangal.

[3]"Secure DCT-SVD Domain Image Watermarking Embedding Dta In All Frequencies." By Alexander Sverdlov, Scott Dexter, Ahmetm. Eskicioglu Dept. of CIS ,Brooklyn College.

[4] "Steganography Technique Based on DCT Coefficients" by Hardik Patel, Preeti Dave Proceeding of IJERA, Issn: 2248-9622 Vol. 2 PP.713-717 Feb 2012.

[5]."Steganography Approach For Hiding image in DCT Domain "By Blossom Kaur ,Amandeep Kaur,Jasdeep Singh Dept. of Computer Science, Muktsar Proceeding of IJAET , V0l.1 ,PP.72-78July 2011. ISSN: 2231-1963.

[6]. "Robust Digital Watermarking Using DWT-DCT-SVD" by Sumit Kumar P .Rajapati, Amit Naik,Anjulata Yadav Dept.of E&TC ,Indore.pracedding of IJERA ISSN:2248-9622,vol.2,pp.991-997 ,June 2012.

[7]. A hybrid DWT-SVD Method for Digital Video Watermarking" by Rathod Jigisha D., Rachana V.Modi.Dept. of Information Technology Proceeding of IJARCCE ISSN-2319-5910,Vol-2. 2771-2775, July 2013.