ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

DCT Domain Video Watermarking Technique for AVI Video

Manoj Kumar[1], Dolley Shukla[2]

M.E.Scholar, Faculty of Engineering & Technology, Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, India[1]

Sr. Associate Professor, Faculty of Engineering & Technology, Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, India[2]

ABSTRACT: As the digital multimedia are integrated via the network, large amount of data is transfer and circulated easily and becoming faster, easier, and require less effort to make exact copies. This progress will benefit multimedia product owners as sales will increase. The major obstruction is the lack of effective intellectual property protection of digital media to put off unauthorized copying and distribution. In this paper we propose Digital video watermarking scheme based on discrete cosine transform also the Design of this scheme using Matlab Simulink. Watermarking technique has been proposed as a method to hide secret information into the signals so as to discourage illegal copying or attest the source of the media.
.

KEYWORDS: DCT, AVI, PSNR, Frame size, Frame rate

I. INTRODUCTION

In analog world, a painting is signed by the artist to attest the copyright, an identity card is stamped by the steel seal to avoid forgery, and the paper money are identified by the embossed portrait.[20] This type of signatures, seals or watermarks have been used from ancient times as a way to recognize the source, creator of a documents or images or pictures. The watermark must be embedded into the media so that the watermarked signal is undetectable by the user. Video watermarking technique is to hide copyright information into video sequence to prevent copy right infringement. [21]

Watermarking can be divided into two types

1) Visible
2) Invisible.

For visible watermarking, the embedded watermark can be visually observed. The advantage of visible watermarking is that it is easy to recognize the owner of the image without any calculation, but its disadvantage is that the embedded watermark can also be easily removed or destroyed.

Invisible watermarking, the embedded watermark cannot be visually observed. It can be classified into two types

1) robust
2) Fragile watermarks.

Robust watermarks are usually designed to resist arbitrary malicious attacks such as image scaling, bending, cropping, lossy compression, etc. fragile watermarks are adopted and designed to detect any unauthorized modification such as distortion under the slightest changes to the data. [22]

Attacks on watermarks

a) **The compression schemes** like JPEG and MPEG degrades the data quality, thus possibly altering the watermark.
b) **Geometric operations** like rotation, translation, scaling and cropping distort data and possibly alter the watermark.
c) **Signal Processing Operations** like D/A, A/D conversion, re-sampling, re-quantization, dithering, linear filtering, non linear filtering etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

c) **Printing and rescanning**, re-watermarking, forgery are some of the intentional attacks which alter the watermark.

Intentional attacks: The intentional watermark attack includes Single frame attacks like filtering attacks, contrast and color enhancement and noise adding attack. Or statistical attacks like averaging attack and collision attack.
Unintentional attacks: The unintentional attacks may be due to Degradations that can occur during lossy copying, or due to Compression of the video during re encoding or because of Change of frame rate and Change of resolution.

The watermark should be embedded into the host signal so that the watermarked signal is undetectable by the user. Likewise, the watermark should be:

a. Undeletable

The watermark must be difficult or even impossible to remove by a hacker, at least without obviously degrading the original signal.[20]

b. Undetectable

A 'pirate' should not be able to detect the watermark by comparing several watermarked signals belonging to the same author. [20]

c. Robust to Lossy Data Compression

The watermark should be surviving the lossy compression techniques like JPEG and MPEG which are commonly used for transmission and storage. [20]

d. Robust to Signal Manipulation and Processing Operations

The watermark should still be retrievable even if common signal processing operation arc applied, such as signal enhancement, geometric image operations, noise, filtering, etc. [20]

e. Unambiguous

Retrieval of the watermark should be unambiguously identifying the owner, and the accuracy of identification should degrade gracefully in the face of attack. [20]

f. Imperceptible

The watermark should be imperceptible so as not to affect the viewing experience of the image or the audio quality of the original signal. [20]

Watermarking techniques can be classify into

1) Spatial domain
2) Frequency domain.

Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame whereas watermarks of frequency domain techniques are applied to coefficients obtained as the result of a frequency transform of either a whole frame or single block-shaped regions of a frame.
Commonly used frequency domain techniques are,
1) Discrete Fourier Transform (DFT),
2) Discrete Cosine Transform (DCT),
3) Discrete Wavelet Transform (DWT).

II. RELATED WORK

Powar et al [8], proposed a matlab Simulink model for watermark embedding for digital video. And proposed that embedded watermark is robust against various attacks that can be carried out on the watermarked video. Due to multi resolution characteristics of DWT this scheme is robust against several attacks. Software model is design by using MATLAB/ Simulink. There is no noticeable difference between the watermarked video frames and the original frames. As a future work this Simulink model can be interface with FPGA by using Xilinx system generator block.

Babu et al [16], proposed a Blind video watermarking algorithm that can resist noise attacks, frame removal, and frame averaging, compression attacks and filtering attacks. Each video frame is divided into non-overlapping 8*8 blocks. Each block is transformed 2D-DCT. After performing the same transformation to all the blocks and frames, 1D

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

DCT is applied to each coefficient on time domain. Now, the quantization is applied to embed the secret logo. Embedding is performed in to DCT intermediate frequency coefficients of the video frame. The DCT intermediate coefficients are adjusted by using a controlling parameter k which is a tradeoff between the perceptual quality and resilience to the attacks.The proposed method gives good results for noise attacks and filtering attacks. For compression attacks, the extracted logo is slightly disturbed, but it is easy to recognize. This scheme is not robust against geometrical attacks like frame rotation. In future, the algorithm can be improved to resist these attacks.

Jigisha D. et al [18], proposed a technique which is Hybrid DW- SVD method for digital video watermarking. This method is divided in 2 parts: embedding watermark and extracting watermark. In embedding and extracting process, they Compare Hybrid Method with DCT method, calculate PSNR ratio, elapsed time and check robustness, imperceptibility of video. This method can be used for authentication and data hiding purposes. The DCT based method is very time consuming though it offers better capacity and imperceptibility. A Hybrid DWT-SVD method is found to be better than DCT method. The new method was found to satisfy all the requisites of an ideal video watermarking scheme such as imperceptibility, robustness and fast processing time.

Sharma et al [1], proposed a comprehensive approach for protecting and managing video Copyrights with watermarking techniques. They propose a novel digital video watermarking scheme based on image LSB watermarking scheme. Robustness and fidelity are the essential requirements of a successful watermarking scheme. They focus on improving the fidelity of the scheme. The fidelity of the scheme is enhanced by applying a LSB watermarking algorithm, which optimizes the quality of the watermarked video. The effectiveness of this scheme is verified through a series of experiments. This technique is tested on uncompressed (taken from AVI high quality film) and uncompressed (taken by digital camera) video movies. The watermark which is embedded into the regions between frames (HL, LH bands). Experimental results show that the proposed new scheme has a higher degree of invisibility and visibility against the attack of frame dropping, adaptive quantization, and frame filtering than the previous developed scheme in spatial domain. The involved parameters are tuned in order to evaluate the performance of the algorithm by using the performance parameters (quality measure and similarity). The future work will be the implementation of our scheme in different compressed video codec standards like (MPEG2, MPEG4). It can also be used for audio layer in video codec standards.

III. PROPOSED ALGORITHM

In this project the methodology which is use is the discrete cosine transform (DCT) algorithm. The discrete cosine transform (DCT) represent an image as an addition of sinusoids of varying magnitudes and frequencies. The 2-D discrete cosine transform function computes the two-dimensional discrete cosine transform (DCT) of an image. The DCT has the property that, for a typical image, most of the visually important information about the image is concentrated in just small coefficients of the DCT. For this reason, the DCT is frequently used in image compression applications. For example, the DCT is at the heart of the international standard lossy image compression algorithm known as JPEG. The name comes from the working group that developed the standard: the Joint Photographic Experts Group. The discrete cosine transforms (DCT) help to divide the image into parts or spectral sub-bands of differing importance with respect to the image's visual feature. The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

The equation for a 1D (N data items) DCT is defined by the following equation:

$$F(u) = \left(\frac{2}{N}\right)^{0.5} \prod_{i=0}^{N-1} A(i)\ \cos\left[\frac{\pi u}{2N}(2i+1)\right] f(i)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

And the corresponding ***inverse*** 1D DCT transform is simple $F^{-1}(u)$, i.e.:

Where

$$A(i) = \begin{Bmatrix} \frac{1}{\sqrt{2}}, for\ \varepsilon = 0 \\ 1\ otherwise \end{Bmatrix}$$

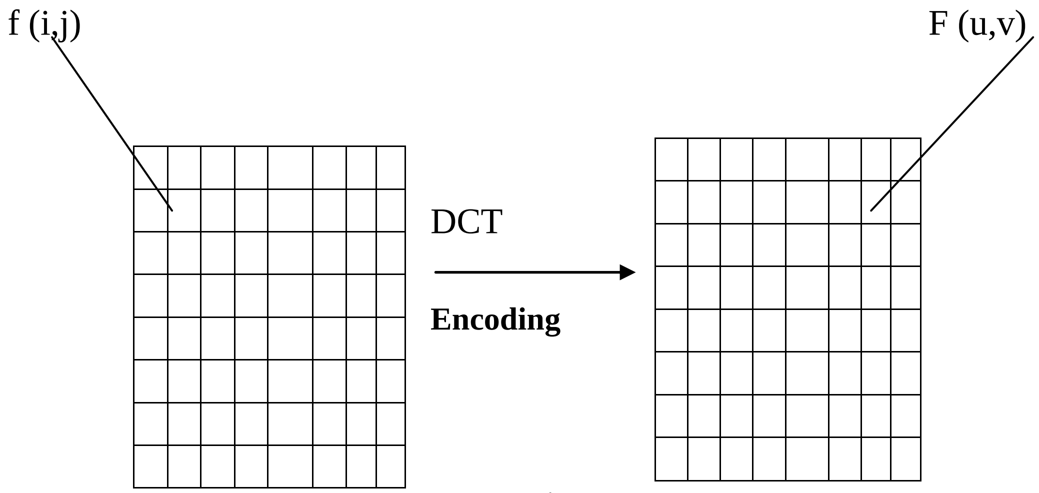


Fig 1

The equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$F(u,v) = \left(\frac{2}{N}\right)^{0.5}\left(\frac{2}{M}\right)^{0.5}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1} A(i)\,A(j)\cos\left[\frac{\pi u}{2N}(2i+1)\right]\cos\left[\frac{\pi v}{2M}(2j+1)\right]f(i,j)$$

And the corresponding ***inverse*** 2D DCT transform is simple $F^{-1}(u,v)$, i.e.:

Where

$$A(\varepsilon) = \begin{Bmatrix} \frac{1}{\sqrt{2}}, for\ \varepsilon = 0 \\ 1\ otherwise \end{Bmatrix}$$

The basic operation of the DCT is as follows:

- The input image size is N by M.
- F (i,j) represent the intensity of the pixel in row i and column j.
- F (u,v) is the DCT coefficient in row k1 and column k2 of the DCT matrix.
- For most images, much of the signal energy lies at low frequencies.
- Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.
- The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level;

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

- 8 bit pixels have levels from 0 to 255.
- Therefore an 8 point DCT would be:

The output array of DCT coefficients contains integers; these can range from -1024 to 1023.It is computationally easier to implement and more efficient to regard the DCT as a set of basis functions which given a known input array size (8 x 8) can be precomputed and stored. This involves simply computing values for a convolution mask (8 x8 window) that get applied The values as simply calculated from the DCT formula. The 64 (8 x 8) DCT basis functions.

Watermark embedding process

The Watermark embedding process consists of the following steps:

1. Original Video is converted into frames RGB frames are converted to Intensity frames.
2. Block processing and 2-DCT is applied on it. .
3. Watermark image converted into intensity image.
4. Maintain image gain value.
5. 2-DCT applies on it.
6. Watermark embedding process is done. The embedding equation is:

$$M_e = M_i + xW$$

Where, x is the watermark embedding strength (Gain).

M_e-Watermarked Video

M_i-Original Video

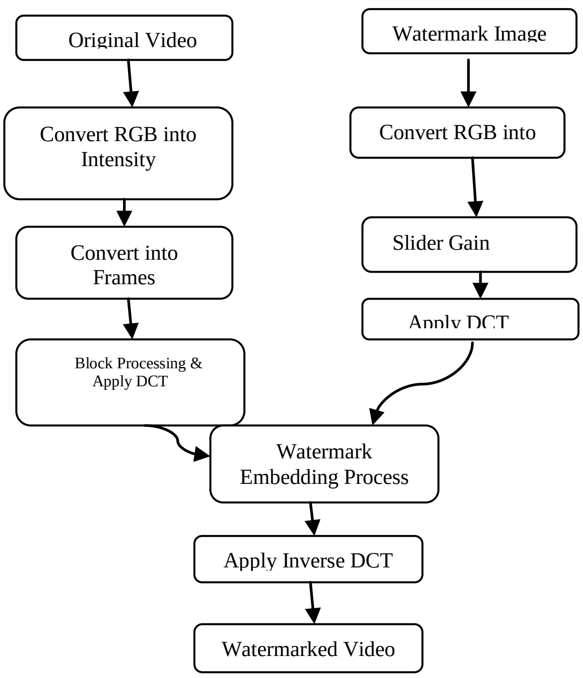
W- Watermark image

7. Inverse DCT is applied to obtain the watermarked video.

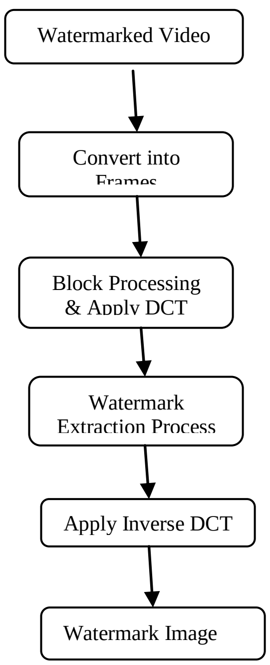
Watermark Extraction Process

The steps used for watermark extraction is the same as the steps in the embedding but in the reverse direction.

1. Watermarked video is converted into frames.
2. Block processing and 2-DCT is applied on it.
3. Following equation is used to extract watermark,
4. Inverse DCT is applied to obtain the watermark image.



Embedding Process



Extraction Process

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

IV. SIMULATION RESULTS

SIMULINK BASED IMPLEMENTATION

Simulink is a block diagram setting and Model-Based Design. It supports system-level design, simulation, automatic code creation, and verification of embedded systems. It provides a graphical editor, customizable block libraries for modeling and simulating dynamic systems. It enables to integrate MATLAB algorithms into models and export simulation results to MATLAB for further analysis.[15]

Here I am using different blocks for embedding watermark into video signal like from multimedia, frame conversion,2-D DCT,2-D IDCT, Gain etc. same block also used for extraction of watermark image.

The experimental results showed that there is no perceptible Distortion in the embedded video. The main advantage of this method is that it is robust. In the experiments, various .avi videos are used as the host whereas .jpg, .bmp & .pnp images are used as watermark images. The performance evaluation of algorithm is summarized in Tables

If different size of images are use as a watermark image than the value of psnr and the average psnr value are shown in below tables. From this tables we have observe that if the size of images is different than we got different psnr value, means if the frame size of watermark image is small than we got high psnr value.

Table-1 Average PSNR value for video 1

Original Video name	Size of input Video	Frame rate	Watermark image	Frame Size of Image	PSNR (in dB)	Average PSNR value (in dB)
Video 1	4.28 MB	10 F/S	Image 1	100*75	43.25	39.242
			Image 2	260*85	39.98	
			Image 3	512*256	33.01	
			Image 4	125*156	40.73	

Table-2 Average PSNR value for video 2

Original Video name	Size of input Video	Frame rate	Watermark image	Frame Size of Image	PSNR (in dB)	Average PSNR value (in dB)
Video 2	15.6 MB	20 F/S	Image 1	100*75	45.16	40.06
			Image 2	260*85	37.38	
			Image 3	512*256	33.73	
			Image 4	125*156	43.98	

Table-3 Average PSNR value for video 3

Original Video name	Size of input Video	Frame rate	Watermark image	Frame Size of Image	PSNR (in dB)	Average PSNR value (in dB)
Video 3	12.6 MB	25 F/S	Image 1	100*75	47.33	42.297
			Image 2	260*85	44.16	
			Image 3	512*256	33.72	
			Image 4	125*156	43.98	

Original Video	Images	Images after passing Gain	Watermarked Video	Extracted Images	PSNR
					43.35 dB
					39.98 dB
					33.01 dB
					40.73 dB

If the watermark image frame size are same than the PSNR value for all three video are also same. From the table you can see that if we use image 1 for all 3 videos than the psnr value for all 3 videos are same. The result for this condition is shown below table.

Table-4 PSNR value for same size image (265*85)

Watermark image	Frame Size of Image	PSNR (in dB)		
		Video 1	Video 2	Video 3
Image 1	260*85	34.36	34.36	34.36
Image 2	260*85	35.83	35.83	35.83
Image 3	260*85	33.35	33.35	33.35
Image 4	260*85	34.98	34.98	34.98

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Table-5 PSNR value for same size image (50*50)

Watermark image	Frame Size of Image	PSNR (in dB)		
		Video 1	Video 2	Video 3
Image 1	50*50	49.69	49.69	49.69
Image 2	50*50	47.17	47.17	47.17
Image 3	50*50	42.2	42.2	42.2
Image 4	50*50	43.58	43.58	43.58

From the above result we can analyse that if we are using small frame size image as compare to large frame size we got better psnr value for small size frame as compare to large frame size image.

V. CONCLUSION

The major obstruction is the lack of effective intellectual property protection of digital media to put off unauthorized copying and distribution. The performance of this watermarking technique defines in terms of psnr. The conclusion of the project is,

- If the watermark image frame size are same than the PSNR value for all videos are also same. From the table you can see that if we use image 1 for all 3 videos than the psnr value for all 3 videos are same. The result for this condition is shown above table.
- From the above result we can analyze that if we are using small frame size image as compare to large frame size we got better psnr value for small size frame as compare to large frame size image.

REFERENCES

[1] Sunil Sharma, Mahendra Kumar Rai and Tanvi Sharma, "An Enhance LSB Watermark Approach for Robustness and Security in uncompressed AVI, Video", *IJETTCS*, Volume 3, Issue 1, January – February 2014
[2] B. M. Macq and J. J. Quisquater, "Cryptology for digital TV broadcasting," vol. 83, pp. 954–957, June 1995.
[3] G. Langelaar, I. Setyawan, and R. Lagendijk. Watermarking digital image and video data. IEEE Signal Processing Magazine, 17:20–46, 2000.
[4] FrankY. Shih∗ , Scott Y.T. Wu "Combinational image watermarking in the spatial and frequency domains" Pattern Recognition 36 pp: 969 – 975, 2003
[5] Juan R. Hernández, Associate Member, IEEE, Martín Amado, and Fernando Pérez-González, Member, IEEE "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure" vol. 9, no. 1, pp:55-68, january 2000
[6] Jun Zhang, Jiegu li, Ling Zhang, "Video water marking Technique in Motion Vector" , 1530-1834/01, pp: 179-182,2001
[7] Athanasios Nikolaidis and Ioannis Pitas, Senior Member, IEEE "Region-Based Image Watermarking" VOL. 10, NO. 11, pp: 1726-1740 november 2001
[8] Yulin Wang and Alan Pearmain, Member, IEEE "Blind MPEG-2 Video Watermarking Robust Against Geometric Attacks: A Set of Approaches in DCT Domain" VOL. 15, NO. 6, pp: 1536-1543, june 2006
[9] A. Piva, M. Barni, F. Bartolini, V. Cappellini "DCT-basedWatermark Recovering without Resorting to the Uncorrupted Original Image", pp: 1-4, 2001
[10] Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva "A DCT-domain system for robust image watermarking", Signal Processing 66,pp: 357-372,1998
[11] Frank Hartung,Bernd Girod, "Watermarking of Uncompressed & Compressed Video", Vol. 66 ,No. 03, may 1998
[12] Raymond b. Wolfgang, student member, ieee, Christine i. Podilchuk, member, ieee, and Edward j. Delp, fellow, ieee, "perceptual watermarks for digital images and video", vol. 87, no. 7, pp: 1108-1126,july 1999
[13] Jing Zhang, Student Member, IEEE, Anthony T. S. Ho, Senior Member, IEEE, Gang Qiu, and Pina Marziliano, Member, IEEE, "Robust Video Watermarking of H.264/AVC", VOL. 54, NO. 2, pp: 205-209, february 2007
[14] A. M. Alattar, E. T. Lin, and M. U. Celik, "Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressed video," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 787–800, Aug.2003.
[15] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad, "Video Watermarking Techniques for Copyright protection and Content Authentication",IJCISIMA, Volume 5, pp. 652–660,2013
[16] D.Niranjan babu, D.Jagadeesh, "A Blind and Robust Video Water Marking Technique in DCT Domain", IJEIT, Volume 2, Issue 2, August 2012
[17] Aditi Agarwal, Ruchika Bhadana and Satishkumar Chavan, "A Robust Video Watermarking Scheme using DWT and DCT", IJCSIT, Vol. 2 (4) ,pp. 1711-1716, 2011
[18] Rathod Jigisha D, Rachana V.Modi, "A HYBRID DWT-SVD METHOD FOR DIGITAL VIDEO WATERMARKING",IJARCCE, Vol. 2, Issue 7, July 2013

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

[19] Chiou-Ting Hsu and Ja-Ling Wu, Senior Member, IEEE "Hidden Digital Watermarks in Images" transactions on image processing, vol. 8, no. 1,pp: 58-68 january 1999
[20] Chiou-Ting Hsu,Ja-Ling Wu, "DCT-BASED WATERMARKING FOR VIDEO",IEEE Transactions on Consumer Electronics, Vol. 44, No. 1, FEBRUARY 1998.
[21] Jun Zhang, Jiegu li, Ling Zhang, "video watermarking technique in motion vector", IEEE, pp.179-182, 2001
[22] Hui-Yu Huang, *Member, IEEE*, Cheng-Han Yang, and Wen-Hsing Hsu, "A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation", IEEE transactions on information forensics and security, vol. 5, no. 4, December 2010

BIOGRAPHY

Manoj Kumar is a ME Scholar in the Electronics & Telecommunication Department, Faculty of Engineering & Technology, Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh, india. He completed his Bachelor of Engineering degree in 2009 from CSIT, Durg, Chhattisgarh, India. Her research interests in communication.