iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Block Based Novel Digital Video Watermarking Scheme Using DCT

Mohini Shinde[1], SadhanaTodkar[2], PradnyaUbale[3], Prof. R.M. Kedar[4]
[1,2,3,4]*KJ College of Engineering and Management Research, Pune University, India*

Abstract: Today, there are lots of facilities such as video on demand, digital music downloads and multimedia social networks through internet which challenges to the design of content protection measures aimed at preventing copyright violations. Digital watermarking has been proposed a brick of such protection systems, which gives an opportunity to embed or hide an image which proves an identity of author and provides a protection to multimedia content. The rapid growth of network distributions of images and videos, it becomes a need for copyright protection against the piracy by using video watermarking (VM).Different digital watermarking schemes have been proposed to address this issue of ownership identification. The video watermark technique is robust against the various attacks by the attacker.
Keywords: Digital watermarking, Discrete Cosine Transform (DCT), Copyright protection

I. INTRODUCTION

Information can be made secure by information hiding process. There are three types viz Steganography, Cryptography and Watermarking. Steganography is concerns about concealing the very existence of information. The purpose of steganography is having concealed the communication between two parties whose existence is unknown to a possible attacker. Cryptography is concerns about the protecting the contents of messages. In cryptography, the original data is converted into secrete code and this conversion is done with the encryption algorithm. At the receiving side, the data in secret code is decrypted and turned back to the original data. Watermarking is hiding information in information. Watermarking scheme can be classified into two categories: Spatial Domain Transform (SDM) and Transform Domain Method (TDM) [1]. The main goal of Watermarking is to hide a message in some audio or video data, to obtain new data, in such a way that an eavesdropper cannot remove or replace message which is hidden in new obtained data [5]. Unlike Cryptography, watermark can protect content even after they are decoded.

II. WATERMARKING

Watermarking is the process of inserting secret information that is watermark into original information. Digital watermarking is the process of inserting secret information into digital multimedia such as image, audio or video [2][4]. A digital watermark is a digital signal or pattern inserted into digital document such as text, graphics or multimedia and carries information unique to the copyright owner. Digital watermarking contain image watermark, audio watermark, video watermark. Digital video watermarking is an extension of this concept. In digital video watermarking, we talk specifically about video watermarking.
There are two types of digital watermarking: visible watermarking and invisible watermarking

A. Visible Watermarking

Visible watermark is a transparent overlaid into an image and is visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection [6].

B. Invisible Watermarking

Invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images [6].
Watermarking techniques are classified as following categories:

1) Spatial Domain Watermarking: In spatial domain watermarking schemes, the watermark is embedded into the host image by directly modifying the pixel value of the host image without causing obvious change in appearance [1]. The main advantage of the spatial domain watermarking schemes is that it is required less computational cost. But this technique is not reliable when subjected to normal media operation such as filtering or lossy compression.

2) Transform Domain Watermarking: In transform domain watermarking schemes perform the domain transformation procedure by using transformation functions such as discrete cosine transformation (DCT), discrete Fourier transformation (DFT), discrete wavelet transformation (DWT), etc. Then, the transformed frequency coefficients are modified to embed the

©IJRASET 2015: All Rights are Reserved

desired watermark [5].

a) Discrete Cosine Transformation (DCT): DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking [5][7]. This paper focuses on block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. The main advantages of DCT over DWT and DFT are less complex, fast, and larger embedding capacity and robustness. It also provides better result with high accuracy.

III. DIGITAL VIDEO WATERMARKING

In digital video watermarking, watermark image is embedded into original video. Digital video watermarking consists of basic three approaches: Watermark embedding, Watermark detection, Watermark extraction. Watermark embedding algorithm uses the public key to make the watermark information embed into the original carrier to get conceal carrier [4].

A. Approach to Watermarking Digital Data

Insertion of watermark

Detection of watermark

1) Insertion Of Watermark: For inserting watermark, a watermark insertion unit uses [9]

Original video

Watermark

We have used DCT algorithm to insert a watermark image into a video. We applied segmentation on video. By applying segmentation, the video frames are separated. Then segmentation on Image will breakdown the image into pixels. The pixel value of watermark image is compared with the value of block of video frame. After that IDCT operation is performed and frames are reconstructed. Two large prime numbers and one co-prime (E) number is given as input to the RSA algorithm to encrypt each video frame. The encrypted frames are combined and the video will be stored on the disk.

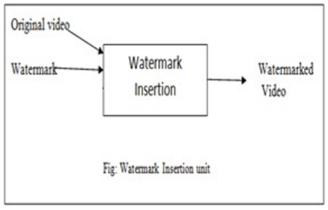


Fig: Watermark Insertion unit

The input video and the watermark are passed through a watermark insertion unit to obtain watermarked video.

B. Detection of Watermark

Detection of watermark consists of:

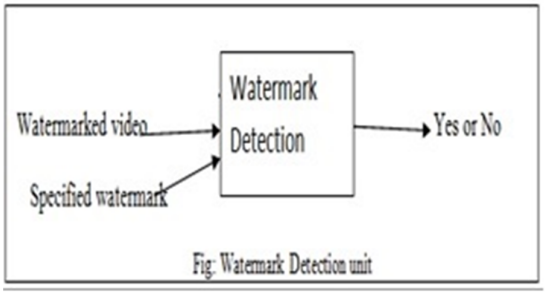


Fig: Watermark Detection unit

In this, watermarked video and watermark image is provided for watermark detection.

Compare it with the original watermark inserted.

The output is authenticity; depending on whether the given watermark matched or not [9].

IV. PROPOSED WATERMARKING SCHEME

The proposed scheme presents an efficient video watermarking technique using discrete cosine transform (DCT) for protection of digital videos [1]. The efficiency of video watermarking technique is achieved with following major steps.

A. Watermark Embedding Process

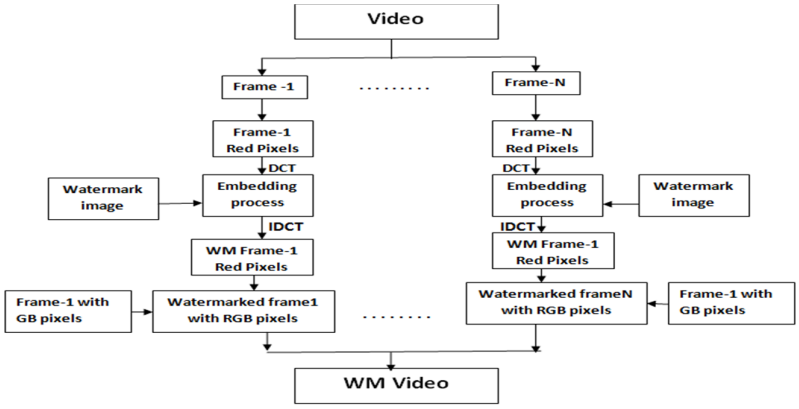


Fig: Watermark Embedding Process

In this process, original video is segmented into frames and then each frame is taken for embedding watermark image. From the video frame, we are taking only r-channel. And that frame's 8*8 pixels block is taken and applied DCT equation (1) to transform into frequency domain. Here we are using middle frequency for embedding image pixels. Now apply embedding algorithm for insertion of watermark image into the frame. And after embedding the watermark, IDCT is applied to the block and converted back to frames which are watermarked.

Embedding algorithm-

The following steps describe the way in which the watermark is embedded in the video.

The video is converted into the number of frames.

Take binary watermark image and take its pixel array.

The r pixels are taken out from RGB frame and are divided into blocks and two-dimensional DCT is applied to the first block.

If the first pixel of watermark image is '255', then it is checked whether (5, 2) is less than (4, 3) or not and if it is not, the two blocks are swapped so as to make (5, 2) < (4, 3).

If the first pixel of watermark image is '0', then it is checked whether (5, 2) is greater than (4, 3) or not and if it is not, the two blocks are swapped so as to make (5, 2) > (4, 3).

Move to the next block and repeat the procedure.

Perform Inverse DCT to have the final watermarked Frame.

The next frame is taken and Steps 3 to 7 are repeated up to the last frame.

All the watermarked frames are combined to make the watermarked video.

B. Watermark Authentication Process

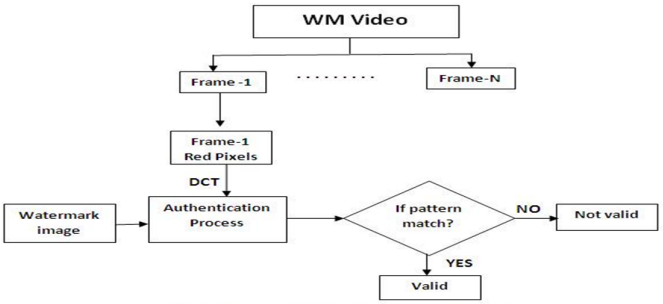


Fig: Watermark Authentication Process

In this process, watermarked video and watermark image is taken as input for authentication. And watermarked video is segmented into frames and taken for authentication. From that frame we will take only red pixels. On that frame apply 8*8 DCT using equation (1). Now extract the image pixel pixels embedded in the frequency domain of the frames and compare the pixel value with the given watermark image pixels. If that pixels matches, then the given watermark image is valid otherwise not.

Above figure shows the video authentication process.

The stepwise execution of the extraction process for the watermark recovery from the video is shown below.
The Video is converted into the number of frames.
Take watermark and convert it into pixel array.
The video frame is divided into blocks and two-dimensional DCT is applied to the first block.
If (5, 2) > (4, 3), then the message bit is 255.
If (5, 2) < (4, 3), then the message bit is 0.
Move to the next block and repeat the procedure.
Compare the extracted pixels with array pixel taken in step 2.
Then take next frame and follow steps 2 to 7 up to the last frame.
If comparison result equals then the video is authenticated.

V. WATERMARK ARCHITECTURE

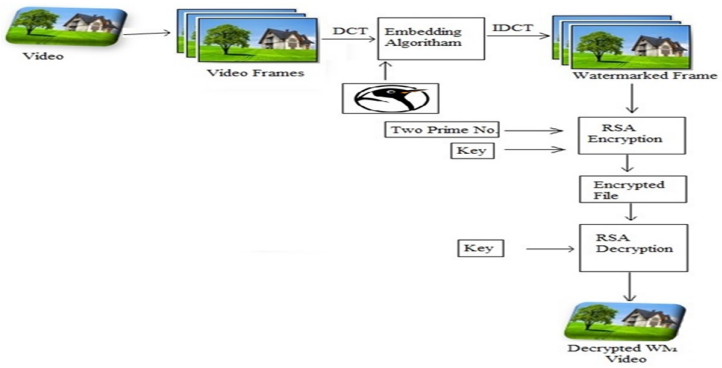


Fig: Watermark Architecture

Above figure shows watermark architecture. In this watermarking scheme involves three algorithms:

A. DCT Algorithm

Discrete cosine transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform. DCT concentrates the information energy in the bands with low frequency, and therefore shows its popularity in digital watermarking techniques. The DCT allows a frame to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of a frame. The middle frequency bands are chosen such that they have minimized to avoid the most visual important parts of the frame (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). Two-dimensional DCT of a frame with size MxN and its inverse DCT (IDCT) are defined in Equations 1 and 2, respectively.

$$f(u,v) = \alpha(u)\alpha(v)\sum_{y=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \cos\left(\frac{(2x+1)u.\pi}{2.M}\right)\cos\left(\frac{(2y+1)v.\pi}{2.N}\right) \quad \text{- (1)}$$

Where u = 0, 1, 2, N-1, v=0, 1, 2, M-1

$$C(u), C(v) = \sqrt{\frac{1}{N}} \quad \text{when u, v=0}$$

$$C(u), C(v) = \sqrt{\frac{2}{N}} \quad \text{when u, v}\neq 0$$

$$f(x,y) = \sum_{V=0}^{N-1} \alpha(u)\alpha(v)\, f(u,v) \cos\left(\frac{(2x+1)u.\pi}{2.M}\right)\cos\left(\frac{(2y+1)v.\pi}{2.N}\right) \quad \text{- (2)}$$

Where x = 0, 1, 2, N-1, y=0, 1, 2, M-1

B. RSA Algorithm

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman [8]. The RSA algorithm is the most commonly used encryption and authentication algorithm.

How the RSA System Works

The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Web site. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key [8]. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key.

C. IDCT Algorithm

Inverse discrete cosine transform (IDCT) algorithm is inverse process of discrete cosine transform. It helps to convert back pixels from frequency domain to spatial domain.

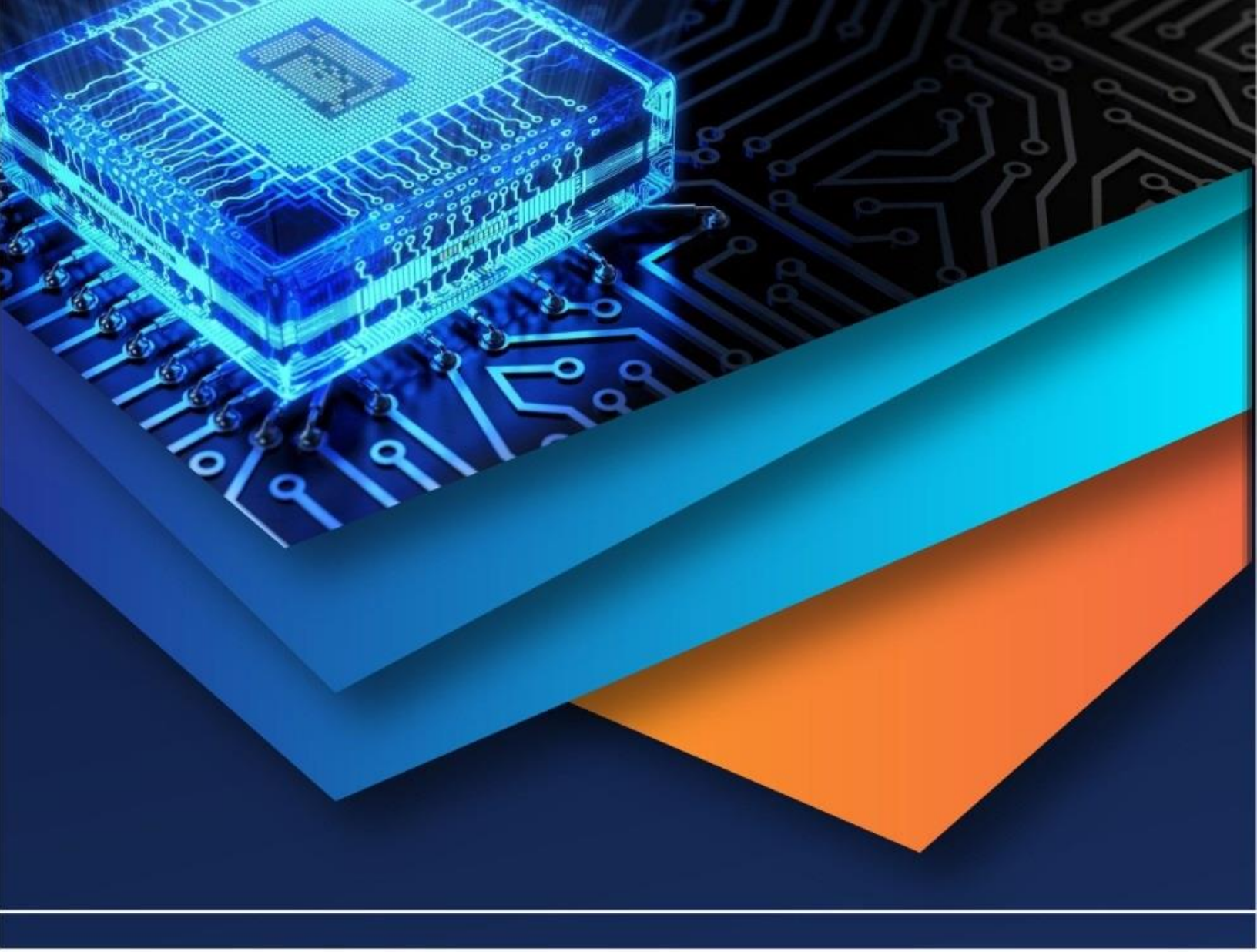
VI. CONCLUSION

The proposed system allows watermarking by using DCT which has larger embedding capacity and provides better result with high accuracy. To protect the video from unauthorized user encryption process is used with the help of RSA. Authentication process is carried out to detect the watermarked Video. Hence it is used for copyright protection and owner authentication one way to discourage illegal duplication.

REFERENCES

[1] “A Block Based Novel Digital Video Watermarking Scheme Using Dct.” Palaiyappan, Raja JeyaSekhar
[2] “A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm.”Chih-Chin Lai
[3] “Survey on digital video watermarking techniques and attacks on watermarks”, International journals of Engineering Science and technology. T. Jayamalar, Dr. V. Radha
[4] “A Survay: Digital Video Watermarking”, International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.Amit Singh, Shusheel Jain, Anurag Jai
[5] “Performance Analysis of Digital Video Watermarking using Discrete Cosine Transform”, Ashish M. Kothari, Ved Vyas Dwivedi
[6]Link “http://www.academia.edu/8836916/Report-121202064929-phpapp02”
[7]Link“http://www.dcis.uohyd.ernet.in/~mravi/downloads/CIP/.../WaterMarking-5Apr06.ppt”
[8]Link“http://www.cse.iitd.ernet.in/~pkalra/siv864/assignment2/DCT-TR802.pdf”
[9]Link “http://www.di-mgt.com.au/rsa_alg.html”
[10]Link “http://www.arnab.org/notes/introduction-to-digital-waterma

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)