www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 11 November, 2014 Page No. 9265-9269

A Block Based Novel Digital Video Watermarking Scheme Using DCT

Mohini Shinde, Sadhana Todkar, Pradnya Ubale

(Computer Engineering, KJ College of Engineering and Management Research, Pune University, India)
(Computer Engineering, KJ College of Engineering and Management Research, Pune University, India)
(Computer Engineering, KJ College of Engineering and Management Research, Pune University, India)

Abstract:

In recent year, almost maximum work is done on internet and many number of images, audios, videos is distributed over the network, so there may be chances to piracy this data and may be chance to perform illegal operation such as duplication, modification etc. So information hiding techniques become more important. For this we are using digital video watermarking scheme. In digital watermarking scheme, some type of digital data such as logo, name or label called as watermark which represent author's ownership are embedded into desire host image. Here adding information to protect copyright, to authenticate, to prevent misuse etc. Afterword watermarked data extracted by extraction process.

Keywords*: Digital watermarking, Discrete Cosine Transform (DCT), Copyright protection*

1. INTRODUCTION

Information can be made secure by information hiding process. There are three types as 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 secrete code is decrypted and turned back to the original data. Watermarking is hiding information in another information. Watermarking scheme can be classified into two categories: Spatial Domain Transform (SDM) and Transform Domain Method (TDM) [1].

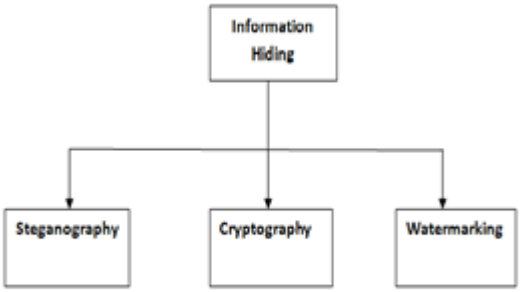


Fig. Classification of Information Hiding [5]

- ***Steganography***

The main goal of Steganography is to hide a message in some audio or video data to obtain new data, in such a way that an eavesdropper cannot detect the presence of message [5].

- ***Cryptography***

Cryptography only provides security by encryption and decryption. But encryption cannot help the seller monitor how legitimate customer handles the content after decryption. Therefore, there is no protection after decryption [5].

- ***Watermarking***

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.

2. 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].

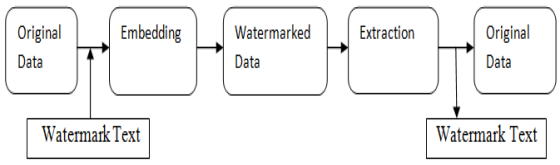


Fig. Watermarking process [4]

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 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:

1.1 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.

1.2Frequency 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 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]. 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.

-The formula used for one dimensional DCT:

$$F(u) = C(u)\sum_{x=0}^{N-1} f(x)\cos\left|\frac{\pi x(2x+1)u}{2N}\right|$$

Where u = 0, 1 ……N-1

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

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

-The formula used for two dimensional DCT:

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

Where u = 0,1,2,…N-1, v=0,1,2,…..M-1

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

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

B) Discrete Wavelet Transformation (DWT)

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy

concentrated in time and are well suited for the analysis of transient, time-varying signals [5].

3. 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].

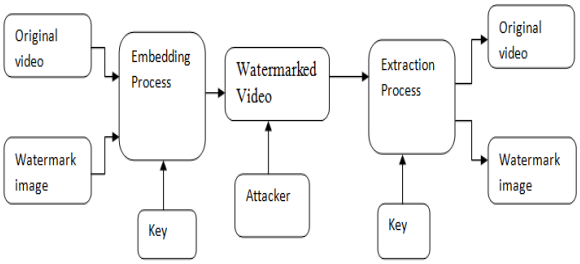


Fig. Watermark embedding and extraction process [4]

Watermark detection or encryption algorithm using the public and private key. The attacker is very difficult to find and modify the hidden watermark data.

i. A Generic Approach to Watermarking Digital Data

1. Insertion of watermark
2. Detection of watermark
3. Removal of watermark

1. *Insertion of watermark*

For inserting watermark, a watermark insertion unit uses [9]

a. Original video
b. Watermark
c. User key

We are using DCT algorithm to insert a watermark image into an video. We are applying segmentation on video. By applying segmentation the video frames are separated. Now we will apply segmentation on Image which will breakdown the image into pixels. Now we will insert each pixel into frames by using DCT algorithm. After that we will combine the frames and we will store the video.
After that we will give 2 primary numbers as input to the RSA to encrypt the video. RSA will encrypt the video and it will be stored on the disk.

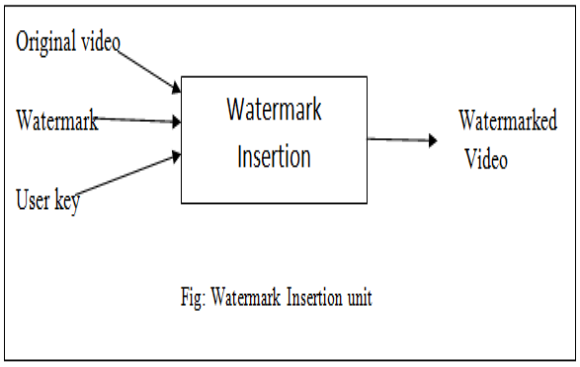


Fig: Watermark Insertion unit

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

2. Extraction of watermark

In extraction of watermark, there are to phases:
-Locating the watermark.
-Recovering the watermark information [9].

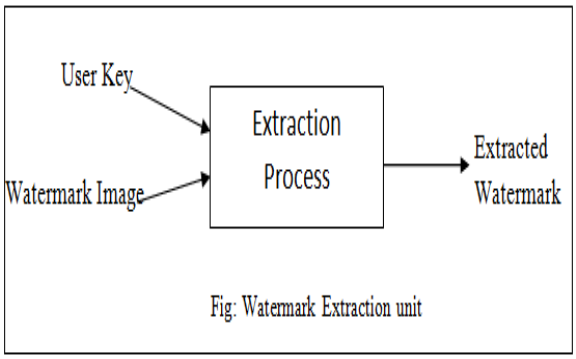


Fig: Watermark Extraction unit

For extracting watermark we need to enter correct RSA key first to start the decryption process. After that we apply IDCT on decrypted video to extract watermark out of it. It is exactly a reverse process of DCT. It will breakdown the video in frames. Then it will extract pixels from the frames using IDCT and it will combine pixels and frames again.

3. Detection of Watermark

Detection of watermark consistsof:

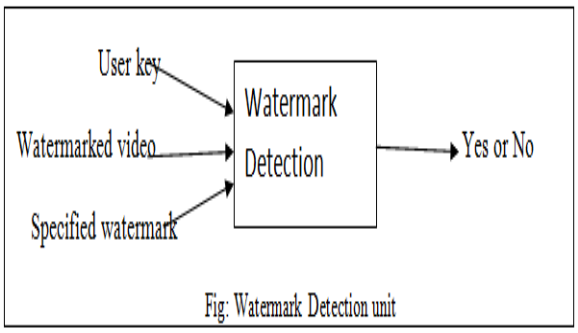


Fig: Watermark Detection unit

-An extraction unit to first extracts the watermark.

- Compare it with the original watermark inserted.

- The output is Yes or No depending on whether the watermark is present [9].

I. 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.

1. Watermark embedding process
2. Watermark extraction process

1. WATERMARK EMBEDDING PROCESS

Before embedding watermark pixels into the input video sequences, the following process should carry out to enhance the security of the hiding information as well as to improve the efficiency of our proposed approach [1]. The process includes,

1) Shot segmentation of video sequences
2) Bit plane slicing of a grayscale image
3) Pixel permutation
4) Decomposition of an image using DCT

1) Shot segmentation of video sequences

The original input video sequence is first segmented into non-overlapping units, called shots that depict different actions. Each shot is characterized by no significant changes in its content which is determined by the background and the objects present in the scene.
Here, we have used Discrete Cosine Transform and correlation measure to identify the number of frames involved in each shot. At first, the first and second frame is divided into a set of blocks of sizes and DCT is applied to every block of the frame.

2) Bit plane slicing of a grayscale image

Bit-Plane Slicing is a technique in which the image is sliced at different planes. Instead of highlighting gray level images, highlighting the contribution made to the total image appearance by specific bits might be desired.

3) Pixel permutation

After the bit plane slicing process, the sliced images are allowed to permute each pixel value to enhance the security of the hiding information. In this scheme, each group of pixels is taken from the image. The pixels in the group are permuted using the key selected from the set of keys. The size of the pixel group is same as the length of the keys, and all the keys are of the same length.

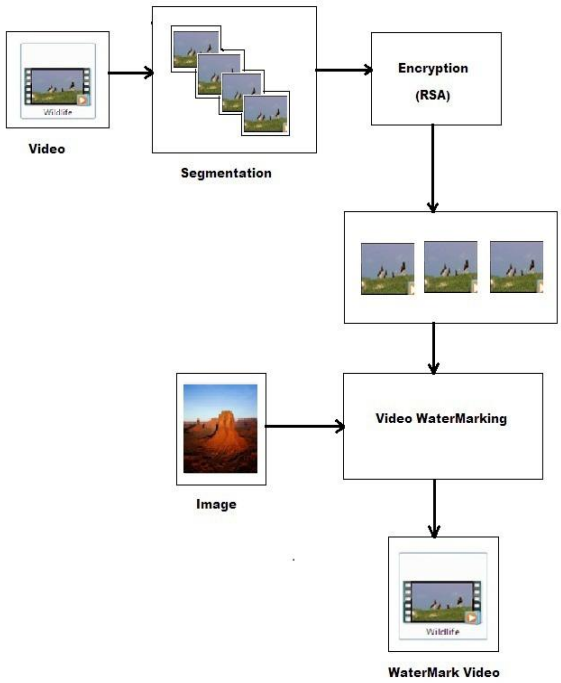
4) Decomposition of an image using DCT

Like other transforms, the Discrete Cosine Transform (DCT) attempts tode-correlate the image data. After de-correlation each transform coefficient can be encoded independently without losing compression efficiency.

2. WATERMARK EXTRACTION PROCESS

After embedding the grayscale watermark image pixels into the original video sequence and extract the embedded watermark image without affecting the original video.

WATERMARK ARCHITECTURE



In this watermarking scheme involves three algorithms:

A) DCT algorithm
B) RSA algorithm
C) IDCT algorithm

A) DCT algorithm

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality) [7]. The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain.

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 and is included as part of the Web browsers from Microsoft and Netscape.

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. Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it.

C) IDCT algorithm

Inverse discrete cosine transform (IDCT) algorithm is inverse process of discrete cosine transform. It helps to combine the part of image into whole image.

CONCLUSION

In this watermarking we are introducing three algorithms such as DCT, RSA, and IDCT. In watermarking the hidden information usually related to cover the object hence it 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]Link "http://www.academia.edu/8836916/Report-121202064929-phpapp02"

[6]Link"http://www.dcis.uohyd.ernet.in/~mravi/downloads/CIP/.../WaterMarking-5Apr06.ppt"

[7]Link"http://www.cse.iitd.ernet.in/~pkalra/siv864/assignment2/DCT-TR802.pdf"

[8]Link "http://www.di-mgt.com.au/rsa_alg.html"

[9]Link "http://www.arnab.org/notes/introduction-to-digital-watermarking