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. 4, Issue 5, May 2016**

# Image Encryption using Video Watermarking Technique

Vasudeva Rao P V, Ankitha K

4th Sem M.Tech, Dept. of Computer Science and Engineering, Sahyadri College of Engineering and Management, Adyar, Mangaluru, India [1]

Assistant Professor, Dept. of Computer Science and Engineering, Sahyadri College of Engineering and Management, Adyar, Mangaluru, India [2]

**ABSTRACT:**Image and Video acts a medium for transmission of Information. Any set of data can be transmitted using image and video encryption techniques without concerning about security. In the proposed work, for transmitting image (i.e. data), a concept called Video Watermarking is used. Watermarking is a technique where a data will be hidden within the multimedia content, thereby ensuing safe transmission of data. The goal of the proposed work is to transmit the data (i.e. image) to the receiver through a multimedia (i.e. video) using video watermarking technique. For achieving this goal, two algorithms namely Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) is used. Also the work is tested on various types of images, various types of videos and the obtained Peak Signal to Noise Ratio (PSNR) are noted. The proposed work can be further expanded by enhancing video watermarking technique for transmitting video through video.

**KEYWORDS**: Discrete Cosine Transform, Discrete Wavelet Transform, PSNR, Video Watermarking, Watermarking

## I. INTRODUCTION

Various factors decide the pace of social development, one among them being the Digital Information being used. Digital Information can be of any type, for e.g. Image, Video, Audio, Text etc. Since the Internet has obtained a tremendous growth, storing, spreading and processing these information have become easy and simple, which have made our life colorful. But in spite of all these advantages, there exist few shortcomings mainly in the form of security of the information being transmitted. There is a high chance that the information we transmit will be corrupted and cracked. At any point, if the information is scaled out, then the producers and the users of the digital information will suffer extensively and be at the receiving end. So now we need to answer a question of how the security of our data can be done during transmission. How the authenticity and integrity of the data can be protected?

In order to answer the above questions and to take care of the security, authenticity and integrity of the data being transmitted, several techniques have been used. Some of them are – Cryptography, Steganography, Watermarking etc. concealed. Cryptography and Steganography techniques have certain disadvantages which are solved using Digital Watermarking method. Digital Watermarking method is introduced in order to overcome the disadvantages. Digital Watermarking, a highly active research area, dates back to early 1990's when it was first introduced. It finds its applications in form of copyright protection, fingerprinting, data authentication, data hiding etc. Now a question arises – What is meant by a watermark? How it is useful in transmitting data? How data will be secured by watermark?

Watermarking is a process of storing information within a digital media – image, text, video or audio, which will be invisible to human eye. Watermarking is a process where a pattern of the secret information will be inserted into a digital media by certain pixel of information from original media. In general, any watermarking scheme proposed, must compulsorily fulfil three basic necessities- 1. imperceptivity which means the distribution of the watermarked image and the original image must be same, 2. resistance against various processing activities such as JPEG compression, cropping, low-pass filtering and so on and 3. security - meaning the competence to prevent the illegal attacks.

Watermarking is performed in two steps. In the first step, embedding is performed, where the secret data will be written into one of the multimedia. Next step is to obtain the secret data from the multimedia, to which is embedded. This is performed by extraction operation, which is the second step. Both embedding and extraction is performed with

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. 4, Issue 5, May 2016

the help of suitable algorithms. In the proposed work, an attempt is made to embed an image (taken as secret data) within a video (multimedia) using Watermarking technique. We employ mainly two algorithms namely Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) for the watermarking process- embedding and extraction process.

## II. RELATED WORK

For any watermarking technique to be effective, the triangle of watermarking requirement- strength, softness and ability has to be satisfied [1]. Peak Signal to Noise Ratio (PSNR) is used as a factor for comparison and is employed at various threshold levels of different images [2]. PSNR value can be improved by subjecting it to blur attack. In DCT watermarking, a new wavelet based image fusion technique was used to improve the strength and hiddenness nature[3]. By improving these attributes, it was found that the quality of the obtained watermarks can be significantly improved. Watermarks can use different kinds of color spaces like YCbCr, CIELAb etc, on which they can be tested[4]. The testing was carried out by subjecting watermarks on various color spaces to different kinds of attacks. Both the color spaces was found to exhibit acceptable results. The proposed watermarking method in [5] uses even-odd quantum for extracting Watermarks, without involving the original video in contrast to other state-of-art techniques. It was noted that compared to DCT, DWT technique offers more security [6]. This is because in DWT, any one of the three sub-bands can be chosen for watermark embedding. Also DWT offers fast and simple way for extracting the embedded watermarks. Using DWT-SVD based color image watermarking technique, a comparative study is made. The study employed various kinds of color spaces namely YUV,RGB and YIQ respectively. By subjecting color spaces to various kinds of attacks, it was found that YUV and YIQ color spaces exhibited high strength compared to RGB.

## III. SYSTEM MODEL

A. *Design Methodology:*

The architecture of the proposed Video Watermarking technique is shown in Fig 1. The main entities involved in this work are – Sender, Host machine and a Receiver. The sender will be selecting a secret image and a cover video. The selected video will be mainly uncompressed, since they can be resized and used according to requirement. If compressed video is selected, resizing cannot be done since its size will be fixed. Once the video is selected, it will be divided into frames. Both secret image and the video frames will be resized. Normally watermarking contains two process- embedding and extraction. Now using either DCT/DWT, the secret image will be embedded into all the frames of the video. This is done because even if some frames of the video is lost, the information can be obtained from the remaining frame(s). After the embedding process is done, all the video frames will be rearranged in sequence in order to produce the original video. All these process will be done by the host machine present in the sender side. Now the obtained video will be containing the secret image within it, which will not be visible to others. the decryption will be performed by the host machine present at the receiver side. Once the decryption is done, the original secret image will be presented to the receiver.

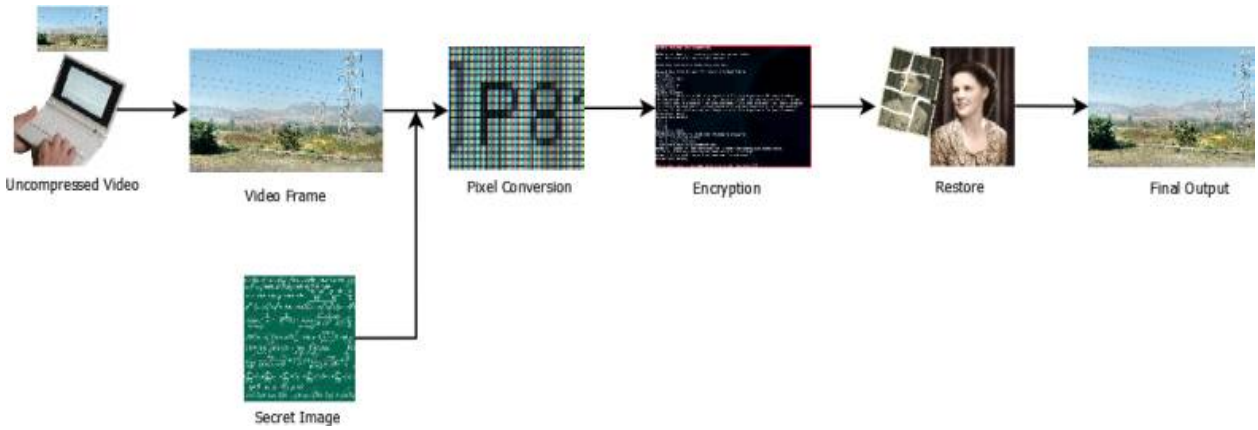


Fig.1. System Architecture

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. 4, Issue 5, May 2016

B. *System Workflow:*

The whole working procedure is mentioned as follows:

1. The sender will select a secret image and a video which acts as a cover for the secret image.
2. Now the host machine present at the sender side will employ MatLab code and will divide the video into frames.
3. The video frame and the secret image will be resized according to the requirements.
4. Using DCT/DWT, the secret image will be embedded within the video frames iteratively.
5. Once embedding is done, the video frames containing the watermarks will be rearranged as per the sequence to regenerate the original video and will be sent to the receiver.
6. The receiver will be knowing exactly which method is used for embedding the watermarks and will employ suitable decryption method for extracting the secret image. Decryption will be done by the host system present at the receiver side.

## IV. EXPERIMENTS

In the proposed work, video watermarking technique is implemented using two algorithms namely –DCT and DWT. Peak Signal to Noise Ratio (PSNR) values are noted for both the results and the graphs are drawn. When DCT was used, mainly gray images were used rather than RGB images. This is because, DCT yields a poor PSNR result for colored frames. For colored frames, we mainly concentrated on DWT technique which yielded better results compared to DCT. Also in DWT, we took a wide range of images having varying qualities like high quality video frame with high quality image, Low quality video with high quality image, high quality video with low quality image and low quality mage with low quality video. Obtained results were noted and accordingly the graphs were plotted.

## V. RESULTS

A. *Result obtained using DCT for Image Encryption:*

A Snapshot of result obtained by using DCT for image encryption is shown in Fig 2. Red circled images represents the secret image, Green circled image shows the video frame, Blue circled frame shows the watermarked image, Pink circled image denotes the extracted watermark image.

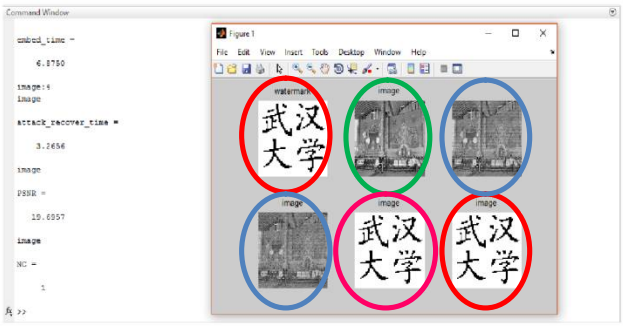


Fig. 2. Image Encryption technique using DCT

B. *Result obtained using DCT for Image Encryption*

A Snapshot of result obtained by using DWT for image encryption is shown in Fig 3,Fig 4, Fig 5 and Fig 6. The snapshots shows the different images considered. In all the snapshots, Red circled image represent the video frames, Green circled image represents the secret image, Blue circled image represent Watermarked image and Pink circled image represent the extracted watermark. Since DWT technique is performed on RGB images, we have considered four cases. Fig 3 shows the case where both video and secret image are of high quality. Fig 4 represents the case where Video is of high quality and secret image is of low quality. Fig 5 represents the case where video is of low quality and secret image is of high quality. Fig 6 represents the case where both video and secret image are of low quality.

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. 4, Issue 5, May 2016

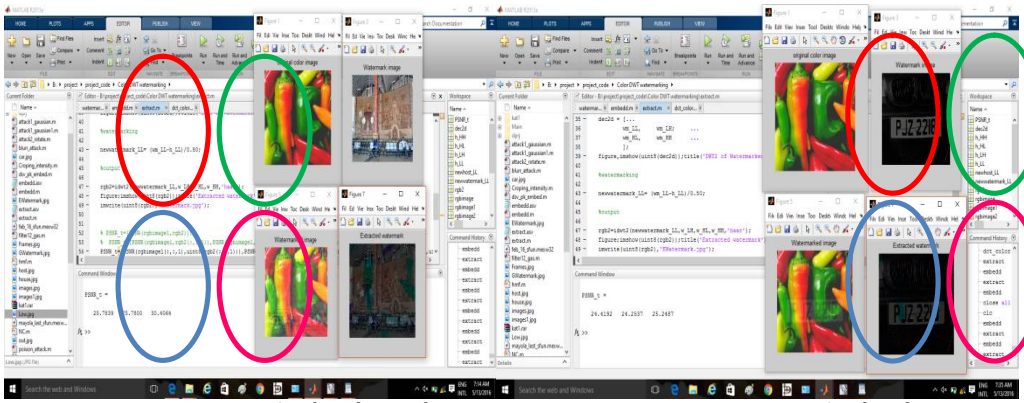

Fig. 3. Image Encryption using DWT (High Video, High Image Fig. 4. Image Encryption using DWT (High Video, Low Image)

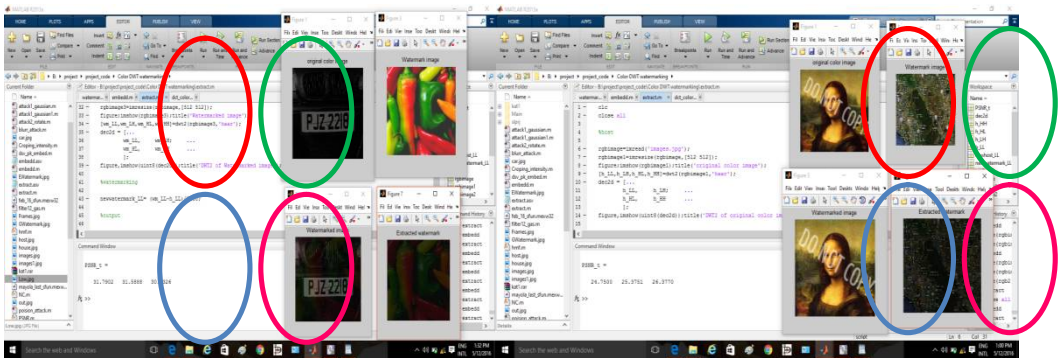

Fig.5. Image Encryption using DWT (Low Video, High Image) Fig.6. Image Encryption using DWT (Low Video, Low Image)

C. *Result Analysis*

The PSNR value obtained from both DCT and DWT Techniques are plotted. Also both the methods were subjected to attacks, with the former one attacked by Poison attack, Rotation attack, Cropping attack, which are shown in the graph in Fig 7. The latter one is also subject to attacks such as Gaussian attack, Rotation attack, Cropping attack, which are shown in Table 1. given below. The PSNR values obtained from DWT for all four cases is shown in Fig.8.

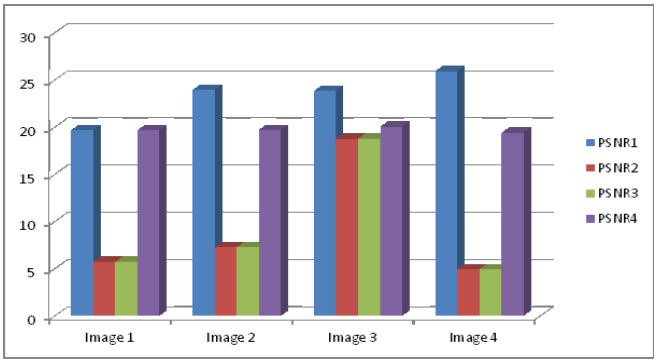


Fig. 7. Image Encryption Technique using DCT

Four images of varying qualities are checked in DCT. The blue colored bar represents the PSNR value obtained during Poison Attack. The Red bar shows the PSNR values obtained during Rotation attack. The Green bar represents the PSNR obtained during cropping attack, whereas the Purple bar represents the PSNR value obtained without any attack.

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. 4, Issue 5, May 2016**

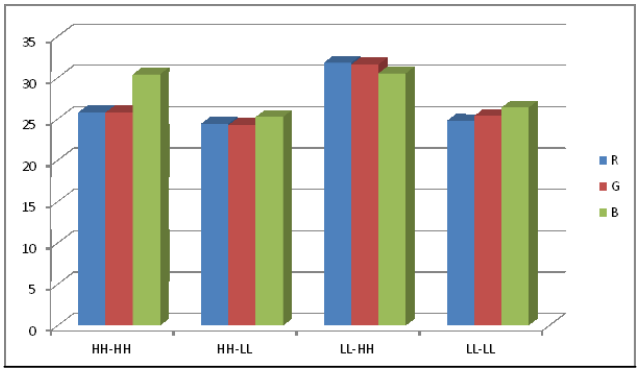


Fig. 8. Performance graph with access cost

Four cases are considered in DWT which are shown in Fig 8. PSNR values of R,G,B Channels of the images are shown in Blue, Red and Green bars respectively. Table 1 represents the PSSNR values obtained when the DWT Technique was subjected to different attacks. PSNR values of R, G, B channels are tabulated separately.

| Attack | Input (Video, image) | PSNR(R) | PSNR(G) | PSNR(B) |
|---|---|---|---|---|
| Gaussian | Host.jpg, Watermark.jpg | 24.42 | 25.05 | 27.18 |
| Rotation | Host.jpg, Watermark.jpg | 26.60 | 27.43 | 28.74 |
| Cropping | Host.jpg, Watermark.jpg | 38.47 | 35.26 | 29.80 |

Table 1. PSNR values obtained from different attacks in DWT

## VI. CONCLUSION AND FUTURE WORK

In the proposed work, an attempt has been made to implement Video Watermarking Technique, where a image is embedded within the video and is transmitted. For implementing this, we have employed two algorithms namely Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). The Peak Signal to Noise Ratio (PSNR) values obtained from both the methods are tabulated and are plotted as a graph. The proposed method is tested using different images and videos having different qualities and the quality of the secret image obtained is determined. Though the concept of video watermarking is proposed, the basic underlying concept is the image-image watermarking, because even in videos, first the videos are divided into frames and then embedding is done into each frame, which is nothing but image-image watermarking. The proposed method can be enhanced by using some better and advanced embedding and extraction algorithms. Also, the proposed Image encryption technique can be refined by making use of high end algorithms for embedding and extraction process. Further, embedding a video within a video can be attempted and the proposed work can be enhanced in the near future.is replicated and stored on to different locations by using replication method. The data is also compressed and stores which minimizes the storage space required. This gives maximum data availability and also greater reliability.

In future for the sake of improving network resource consumption, resource usage de-duplication method can be supported to enhance the performance of the system.

## REFERENCES

1. Ranjan Kumar Aryaet. al.,"A Secure Non-blind Block Based Digital Image Watermarking Technique Using DWT and DCT" In: International Conference on Advances in Computing, Communications and Informatics, pp. 2042-2048, 2015.
2. RakhiDubolia et.al., "Digital Image Watermarking by using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison based on PSNR ", In: International Conference on Communication Systems and Network Technologies, pp.593-596, 2011.
3. F. Arnia, "Perceptual Improvement of Robust DCT-Domain Watermarking through Wavelets Based Image Fusion",In:9th Asia-Pacific Conference on Communications, pp.505-509, 2003
4. SimranjeetKauret. al., "Comparative Analyses of YCbCr Color Space and CIELab Color Space Based On DWT and SVD", In: 1st International Conference on Next Generation Computing Technologies, pp.874-878,2015.

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. 4, Issue 5, May 2016**

5. Tuan Thanh Nguyen and DuanDinh Nguyen, "Robust Blind Video Watermarking in DCT Domain Using Even-Odd Quantization Technique", In: International Conference on Advanced Technologies for Communications, pp.439-444, 2015.
6. S.Tripathiet. al., "Novel DCT and DWT based Watermarking Techniques for Digital Images ", In:18th International Conference on Pattern Recognition, pp.358-361,2006.

## BIOGRAPHY

**Mr. Vasudeva Rao P V**is a 4th Sem M.Tech (Computer Science and Engineering) student of Sahyadri college of engineering and management, Adyar, Mangaluru, India. His research interests are Image Processing, web 2.0, Cloud Computing etc.