Secured Digital Video Authentication System

Aldrina Christian[1], Ravi Sheth[2]

[1]M. Tech. Student, Department of Information Technology, Raksha Shakti University, Ahmedabad, Gujarat, India
[2]Asst. Prof. Department of Information Technology, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

Digital Video is very important in day to day life. There is a problem of illegal updating or manipulation of digital video. There are many techniques to prevent this issue like copyright, Digital Signature and Watermarking. Watermarking is a process of embedding a watermark into a video using the method of discrete cosine transform (DCT) and discrete wavelet transform (DWT).In this paper DCT method is used. In watermarking secret data can be embedding into a video during embedding process. But still there are issues of tampering the video. Tampering like adding frame, dropping frame, replacing frame etc. There are many algorithms of protection. Protection means changing the original data by converting the original data into some unknown form. Cryptography is one of the best techniques to protect image or video. In cryptography there is a term called encryption and decryption. Encryption means change the originality of image or video and decryption means to revert back the originality. Algorithm of encryption, decryption and DCT watermark is present in this paper.

Keywords: Digital Video, Watermarking, tampering, Frame, Cryptography, Encryption, decryption, DCT, DWT, Algorithm.

I. INTRODUCTION

Video processing is one of the best events of action, motion, activity processing. Now video development is increasing in demand. Video processing are used in video conferencing, video Broadcast, making CD, DVDs and TV With the use of internet people can watch video online and download that video too. Digital video is made up of many technology available today like digital camera, CCTV, mobile etc. Videos can be shared by people on social media website and YouTube and many other digital media [1]. You can see video are also used in advertisement on website pages and in pop up also. This video processing needs stream processing in which video frames and streams are processing one by one. So it is risky that someone should tamper the video for their personal interest. There is a black side of video processing like misrepresentation of data, false data of information, modification of data, and this modification of data is called tampering of data [1]. In video tampering a person or attacker can attack on original video and change the originality of video and make a fake video. And their objective is only damaged the original video. Tampered video is also called fake video or doctored video [1-4]. A digital watermark is the process of embedding secret data inside the video or any data. Digital watermark is used to confirm the authenticity of data or integrity of data which is displayed the uniqueness of its owners. Still there are problems of tampering video's frame like adding frames, dropping frames and replacing frames and these all are called modification of frames. Authentication of digital video means we have to verify that the original video's frame is same as the received video, the quality of video. Some attacker can delete some frames in video and then insert the same number of frame inside the video so the receiver cannot determine that the video is forging or not [5]. Now, here encoding and decoding comes into the picture. These encoding and decoding is also called encryption and decryption of data in cryptographic terms [6]. Encoding means to change the originality of video and decoding means to revert back the original video. Sender can encode the secret data and then sent to the other party and the receiver can decode the data [6-8]. So receiver can get original video. And next apply DCT watermark to the encrypted video [9-12]. Here in this paper encrypt the watermark and then embed into the video.

II. PROPOSED SECURED WATERMARK TECHNIQUE

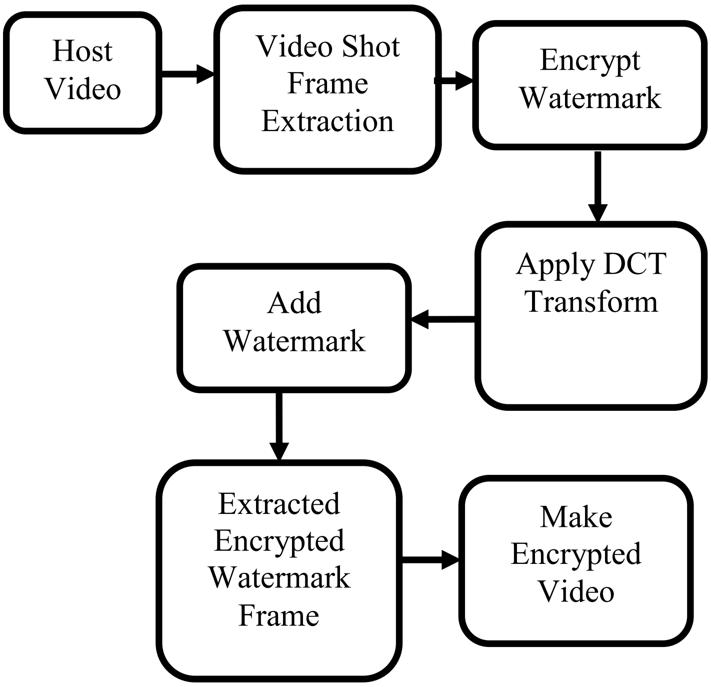

Figure 1. Secured watermark Technique

This section describes proposed secure digital watermarking technique based on DCT (Discrete cosine transforms). First we can convert our video into frames. Encrypt the watermark and then embed into the video. The proposed watermark embedding process including frame extraction, encrypt the watermark, apply DCT transform. Next extract is the encrypted watermark frame and building an encrypted video.

1. Extraction of Frame

Videos are made up of continuous frames. And these contiguous frames are called video shot. So first we have to extract the frame from the video.

Figure 2. Extraction of video frame

2. Video Tampering

There are many types of video tampering like adding frames, dropping frames, replacing frames, swapping frames etc.

A. Adding Frames:

In addition of frames attacker can add one or more frames inside the video. Frames can be taken from the same video or different videos also. So your original video is tempered by adding frames.

B. Dropping Frames:

In dropping of frames attacker can drop one or more frames from the video. And video length is decreased because of dropping frames. And your video is tempered by dropping the frames.

C. Replacing Frames:

In replacing frames attacker can delete one or more frame from the video and replace that frame by some other frame. So your video is tempered.

D. Swapping Frames:

In swapping frames attacker can swap the frames like the second frame goes to tenth position. So your frames are misplaced and this way your video is tampered.

3. **Encrypt the Watermark**

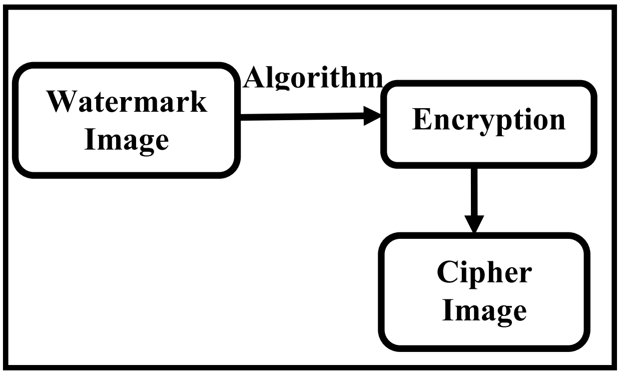

Figure 3. Scheme of Encrypt the watermark

Cryptography is use to make data secret like encryption. In encryption we use some specific algorithm. Video is made up of frames. And frames are contiguous images. Images are made up of pixels. Each pixel has many shades of RGB and GREY. RGB pixel is for color and GREY pixel is for grayscale. For example if it is an 8 bit grey scale image there is 256 shades per pixels. Hence the larger number of bits the more shades of gray to represent an image pixels. Suppose you want to encrypt an 8 bit grayscale image. You required an algorithm for you have to be encrypting the image.

Algorithm for Encryption:

Step 1: Start
Step 2: Select the image
Step 3: Select the size of the image.
Step 4: Change the pixel
Step 5: Apply random permutation of the pixel of the image. Apply pseudo random function.
Step 6: Change the shape of your image
Step 7: Your image is encrypted.

Now you have to embed this encrypted image into your video. Apply DCT to your watermark. And your video is secured with encrypted DCT Watermark. Export the video.

4. **Rebuild the Encrypted Frame**

Now all the frames are encrypted with algorithm and DCT transform watermark and next rebuild all the frames. And make a new encrypted video. This encrypted video is transmitted.

5. **Decrypt the Video Frame**

Receiver receives encrypted video. How we can get original video. There is some algorithm or key to decrypt the video. Receiver would decrypt the video using following algorithm.

Algorithm for Decryption:

Step 1: Import the video
Step 2: Apply random permutation
Step 3: Extract the channel
Step 4: Change the shape
Step 5: Sort the rows
Step 6: Your image is decrypted.

Now apply the inverse DCT to your image. Collect all the frames. Next build new video and this video is same as original video.

III. RESULTS

This secured video authentication work done in MATLAB R2015a. First we would take the video and then extract all the frames. Next we would take an image and apply the encryption algorithm. Then apply Discrete Cosine Transform. And add this watermark into the video's frame. So we would get encrypted frame. And we would build the encrypted video. This encrypted video is transmitted. At the receiver end, receiver would decrypt the video. Apply inverse Discrete Cosine Transform. And retrieve back the original video. The images show the results of secured digital video authentication system.

Figure4. Original Video Frame

This figure shows the one of the original video frame.

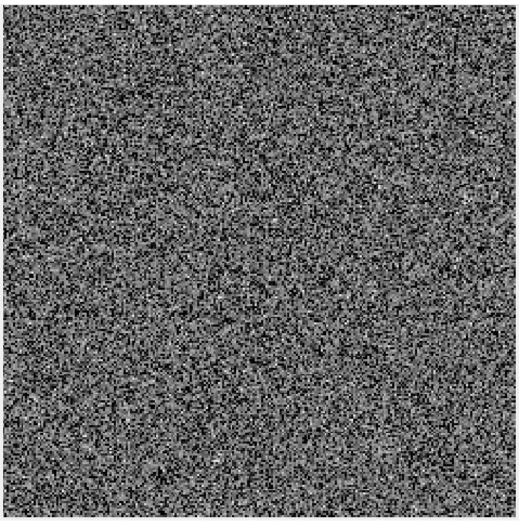

Figure5. Encrypted Watermark

This figure shows the encrypted watermark of an image.

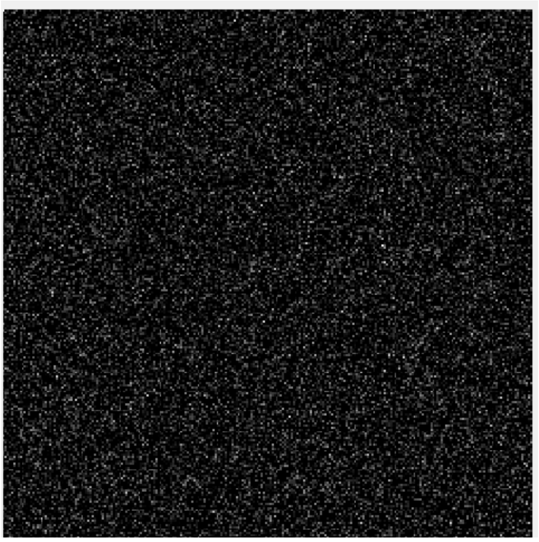

Figure6.DCT Encrypted Watermark

This figure shows the DCT encrypted watermark image.

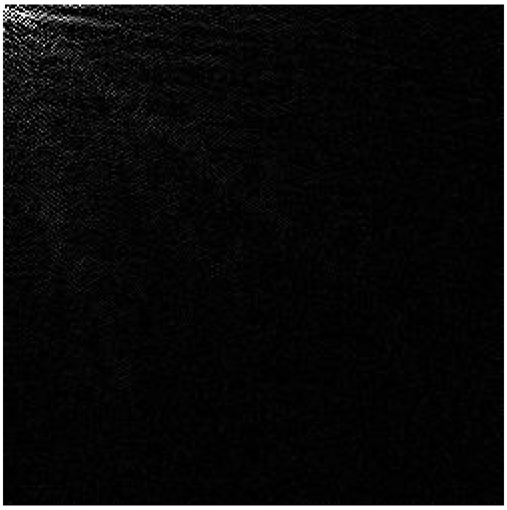

Figure7. Final Encrypted Frame

This figure shows the final encrypted frame.

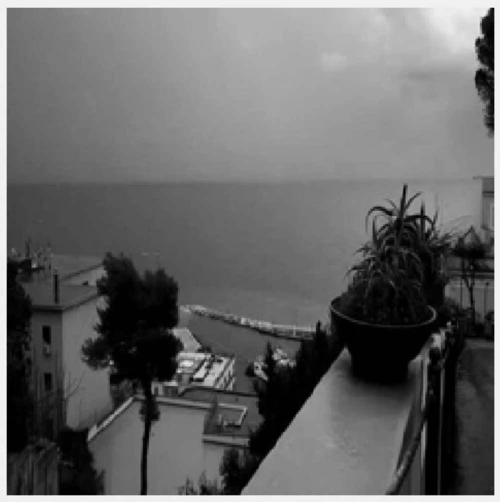

Figure 8. Decrypted Frame

This figure shows one of the decrypted frames of the video. According to the implementation of the digital video authentication system, the proposed method is proved.

IV. CONCLUSIONS

This paper proposed authentication of forensic operation like tempering operation on digital video when frames are added, dropped or replaced. For that we have to add watermark inside the video for security concern but still the issue arise. So this paper has to propose one more security purpose with the help of cryptography. Encrypt the watermark using specific algorithm. And that watermark transform using discrete cosine transform. This secured watermark has to be embedding inside the video's frame. So our frames are encrypted and all encrypted frames are collected and made a new video and transmit the encrypted video. At the receiver end receiver decrypt using specific algorithm. And get the original video. The secured authentication of video watermarking scheme is successfully implemented in MATLAB R2015a.

V. REFERENCES

[1]. Aldrina Christian, Ravi Sheth, "Digital Video Forgery Detection and Authentication Technique - A Review" in IJSRST International Journal of Scientific Research in Science and Technology, Volume 2 Issue 6, November-December- 2016, pp. 138-143, Print ISSN: 2395-6011, Online ISSN: 2395-602X.

[2]. A. Rocha, W. Scheirer, T. Boult, S. Goldenstein, "Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics", ACM Computing Surveys (CSUR), Volume 43 Issue 4, October 2011, Article No. 26, doi: 10.1145/1978802.1978805.

[3]. Wang, W., "Digital video forensics," Ph.D. dissertation, Department of Computer Science, Dartmouth College, Hanover, New Hampshire, June 2009.

[4]. Saurabh Upadhyay, Sanjay Kumar Singh, "Video Authentication: Issues and Challenges" in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012 ISSN (Online): 1694-0814.

[5]. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double MPEG compression," in ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006.

[6]. Mayanak Mishra, Prashant Singh, Chinmay Garg "A New Algorithm of Encryption and Decryption of images using chaotic mapping" International Journal of Information and computation technology Volume No.4, Issue No.7, 2014.

[7]. Vikas Agarwal, shruthi agarwal, rajedh deshmukh "Analysis and review of encryption and decryption for secure communication" International Journal of scientific engineering and research, February , 2014

[8]. Anju,Babita, Reena and Ayushi Aggarwal "An Approach to improve the data security using encryption and decryption techniques" , international journal of information and computation technology,2013

[9]. J. Xu, Y. Su, and Q. Liu, "Detection of double MPEG-2 compression based on distributions of DCT coefficients," International Journal of Pattern Recognition and Artificial Intelligence, vol. 27, no. 01, p.1354001, 2013.

[10]. Ching-Yung Lin, "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection," Ph.D. Thesis, Columbia University, Dec. 2000

[11]. Chih - Hsuan Tzeng, Wen-Hsiang Tsai, "A new technique for authentication of image/video for multimedia applications". MM&Sec 2001: 23-26

[12]. Jamal HUSSEIN1 and Aree MOHAMMED2, "Robust Video Watermarking using Multi-Band Wavelet Transform", IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1, 2009.