Qualitative APPROACH for Data Security, Encryption using Video Watermarking

Jacklin Michael[1], Bastian Babu[2]
[1]Computer Science Engineer, Kerala, India
[2]Assistant Professor, METS School of Engineering, Computer Science Department, Kerala, India

Abstract

The access to unauthorized users is avoided by providing the security through watermarking which is done by video. The digital watermarking process uses watermark embedding technique that hides the information to be communicated. In today's scenario, the communication of multimedia files gets increased over a network. Hence, to protect these kinds of multimedia files from unauthorized access or tampering is a necessity. The authenticity of owner is determined by watermark technique. Then using de-watermarking technique the authenticity is recovered. Better security for multimedia files is provided by video watermarking and against unauthorized access. Double security is provided to multimedia files.

Keywords — *input signal, data encryption, multimedia files, unauthorized access, authentication, video watermarking.*

I. INTRODUCTION

The evidence of authenticity is provided by the watermark, in the form of image or text which is impressed onto the document. Watermarks are of two types : 1) visible watermark 2) invisible watermark. Here, in the project, watermark on image is implemented. The robustness to various attacks is the consideration to different watermarking schemes. The implementation of invisible watermarking (least significant bit) is done in this project. The robustness is increased by watermarking dependency on the original image, at the same time have to make sure the imperceptibility of the watermark. Fragmentation of video into different parts is done. The watermark image is embedded with each fragment. All images that are watermarked after embedding is combined into single unit and it is send to the destination. Some techniques are applied to de-watermark the video at the destination end. While doing so without any attack or misuse the multimedia files are transferred to the other end.

II. RELATED WORK

In [1] authors implemented digital watermarking hardware in which real time insertion of invisible watermark into compressed video. Pipeline structure and parallelism is used in system architecture to increase performance. The proposed system has increased processing speed, increased reliability, low cost, low power consumption. In [2] in order to protect the copyright protection of digital images Discrete Cosine transform (DCT) based video marking technique is used. The video watermarking efficiency is achieved using two steps : i) process of watermark embedding ii) process of watermark extraction. In [3] authors introduced improved version of SHA-1 algorithm, which is applied in FPGA. Using Quartus II the compilation is done and function modules are generated.

III. PROPOSED ALGORITHM

A. Considerations in Design

At sender's end :

- Start.
- Input data.
- Watermark image/video is finalized.
- Encryption on image is done using SHA-2 algorithm.
- Using DCT algorithm watermark image/video is embedded into data.
- Send the data.

At receiver's end :

- Extraction process (i.e. IDCT algorithm) is used to extract the watermark video/image.
- Image is decrypted.
- The key is checked with extracted image using SHA-2 algorithm.
- The data is authenticated if it matches the key.

B. Description of Proposed Algorithm

Using RSA and SHA-2 algorithm, the proposed system provides authentication of multimedia data and files. The proposed algorithm has following steps.

Step 1 : watermark video/image is finalized
Input the data that has to be send. After getting the data watermark image/video is finalized. Then that watermarked video is divided into number of frames.
Step 2 : Using SHA-2 algorithm the image which is finalized will be encrypted.
Step 3 : Watermark image/video is embedded. After dividing the video into number of frames, will embed the watermarked video into data which is to be send over a network using SHA-2 algorithm.
Step 4 : Watermarked video/image is extracted.
After receiver receiving the data, will extract the watermarked video using IDCT algorithm.
Step 5 : The image is decrypted.

The decryption of image is done after extracting the image.

Step 6 : Check the match with the key

The match is checked with the extracted video and the key video which is with receiver. If both the video gets matched, then the received data is not tampered and its authenticity is proved.

IV. PSEUDO CODE

Step 1: The watermarked image/video is generated.

Step 2: Encryption on image is done.

Step 3: The data which is to be send is embedded with the watermarked video.

Step 4: The image is decrypted once received at the receiver's end.

Step 5: The watermarked video is extracted.

Step 6: The watermarked video with the receiver's key video is checked for match.

If (matched)

Original data is received.

Else

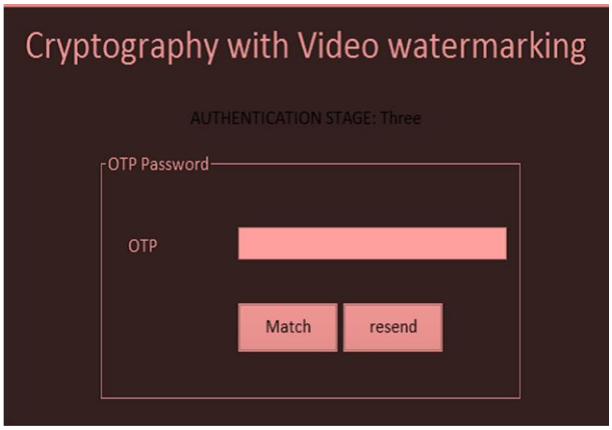
Data is tampered.

Step 7 : End

V. THE RESULT OF SIMULATION

The framework separates the video in edges and the edges are watermarked with another image that is chosen by client. In getting wake of watermarked picture it will scramble and will send to server. The message is unscrambled at the season of enlistment and dewater imprint it and match with the framework. The client will get login into the framework if the match is discovered.

The following Graphical User Interfaces used in the project shows the flow of different authentication stages. Here, cryptography with watermarking has three authentication stages. In each stage it has particular authentication to be performed. In first authentication stage, user has to login with username. If the user is no longer a user and want to login, has to sign up for new user login. In the second authentication stage, video/image is embedded. The OTP has to be entered to check the match . The following are the GUI's of this project.



VI. CONCLUSION

In following areas watermarking can be used: Corporate/commercial world, education, Defense services, secret information sharing. For owner authentication and for copy right protection watermarking scheme is used in order to prevent the attackers. Inserting information known as watermark in potentially vulnerable data discourage illegal duplication.

ACKNOWLEDGMENT

We express our gratitude to the faculty members of Department of Computer Science and Engineering, University of Calicut, Kerala for assisting to develop the project.

REFERENCES

[1] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander fish, Orlyyadid- Pischt, ' Implementation of Digital watermarking system for Video authentication ' , IEEE Transactions on Circuits and System for Video Technology, volume 23, number 02, February 2013 .

[2] Raja JeyaSekhra, Palaiyappan ,'A Block Based Novel Digital Video watermarking Scheme Using DCT', IOSR journal of Electronics And Communication Engineering, volume 5 issue 2 (March – April 2013), pp. 34-44, 2013.

[3] Cheng Xiao Hui, Deng Jian-Zhi,'Design of SHA Algorithm Based on FPGA', 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010