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. 3, Issue 10, October 2015

Data Authentication and Security Using Video Watermarking

Ritesh Bagalkoti, Heena Sheikh, Ankita Pawar, Nikita Dhawade

Professor, Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India

B.E. Student, Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India

B.E. Student, Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India

B.E. Student, Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India

ABSTRACT: Nowadays, there is rapid growth in Communication and spreading of multimedia files over a network. Due to this there is a need to protect this multimedia against any kind of tampering. To provide security from unauthorized access we are using video watermarking. Digital Watermarking is a process to hide information using watermark embedding technique. Watermark technique is used to determine the authenticity of owner. And then the watermark is recovered using watermark extraction technique. Video watermarking is more secured against unauthorized access and provides better security for any multimedia files.It is more robust.

KEYWORDS: carrier signals;encryption; multimedia files;unauthorized access;video watermarking;

I. INTRODUCTION

Everyday tons of data or digital media is distributed over a network. The distributed data can be easily replicated without any error, which can put their owner at risk. To protect the data, different encryption techniques were introduced. The different techniques are: Cryptography, Steganography and Watermarking.

Cryptography is a technique where data is converted into different form and only person with key can decrypt it. But later on it became very simple to decrypt a cipher text. So more complex ways are generated for encryption, which led to discovery of steganography and watermarking. Steganography is a process of concealing a secret message into a file such that outsiders are unknown to the fact that some secret message is hidden inside the file. Watermarking is used to hide information and mainly used to determine authenticity of owner.

There are two types of watermarks: visible watermark and invisible watermark. In this project we are using invisible watermark due to its robustness to various attacks.

The main purpose of this project is to provide security for distribution of multimedia or normal files over a network. Video watermarking technique is based on three steps: i) segmentation of video i.e divide video into number of frames ii) use watermark embedding technique on every frame iii) recover watermark using watermark extraction process.

II. RELATED WORK

In In [1] authors used efficient video watermarking technique using Discrete Cosine transform(DCT) to protect the copyright protection of digital images. According to authors it has a larger embedding capacity and robustness. They achieved a efficiency of video watermarking using two steps: i) watermark embedding process ii) watermark extraction process.

In [2] authors proposed a hardware implementation of digital watermarking that can insert invisible watermark into compressed video in real time. To increase performance, system architecture uses pipeline structure and parallelism. The proposed system features low power consumption, low cost, high processing speed and high reliability.

In [3] authors presents an improved version of SHA-1 algorithm, improved and used in FPGA. QuartusII is used to compile and generate function modules.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

At sender's end:

- Start
- Take data
- Finalize watermark video/image
- Do encryption on image using SHA-1 algorithm
- Embed watermark video/image into data using DCT algorithm
- Send the data

At receiver's end:

- Extract the watermark video/image using extraction process i.e. IDCT algorithm
- Decrypt the image
- Match the key with extracted image using SHA-1 algorithm
- If matched then the data is authenticate
- End

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to provide security and authentication of files or multimedia data using RSA and SHA1 algorithm. The proposed algorithm is consists of following steps.

Step 1: finalize watermark video/image
Take the data which is to be send. Then finalize the watermark video/image. watermarked video is divided into number of frames.

Step 2:
The finalized image will be encrypted using SHA-1 algorithm.
Step 3: embedding the watermark video/image:
Once the video is divided into frames, then using SHA-1 algorithm we will embed the watermarked video into data which is to be send over a network.

Step 4: Extracting the watermarked video/image
Once the receiver receives the data, using IDCT algorithm we will extract the watermarked video.

Step 5: Decrypt the image
After extracting the image the decryption will be done.

Step 4: Match the Key
After extracting the video, that video is matched with the key video which is with receiver. If both matches then the received data is not tampered which proves its authenticity.

IV. PSEUDO CODE

```
Step 1: Generate the watermarked video/image.
Step 2: Do encryption on image
Step 3: Embed the watermarked video into data which is to be send.
Step 4: Once received at the receiver's end, decrypt the image
Step 5: Extract the watermarked video
Step 6: match the watermarked video with the receiver's key video.
        If (matched)
                Received data is original.
        Else
                Data is tampered.
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

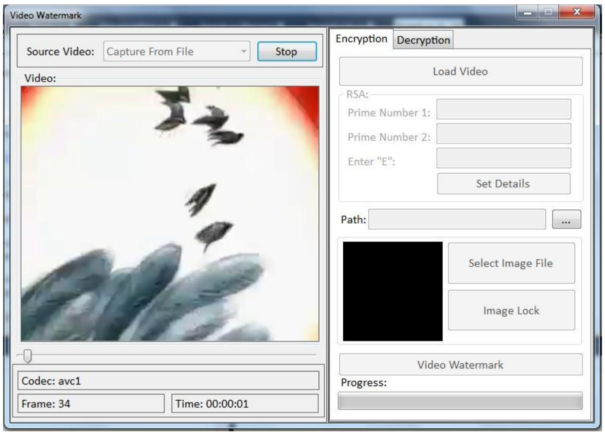
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Step 7: End.

V. SIMULATION RESULTS

The system will divide video in frames and watermark that frame with another image which is selected by user. After getting watermarked image it will encrypted and will send to server.
At the time of registration it will decrypt the message and dewater mark it and match with the system .If match found user will get login into the system.



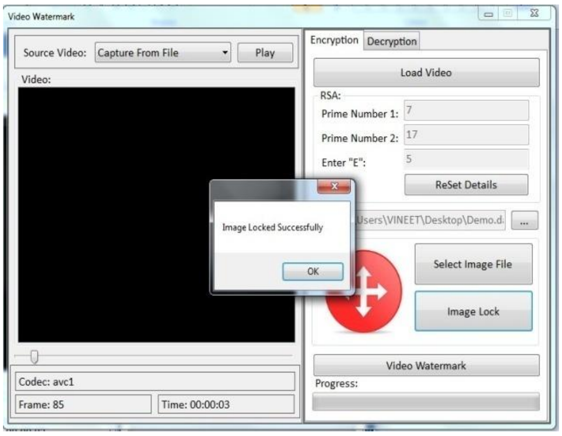
Source Video: Capture From File

Codec: avc1

Frame: 34

Time: 00:00:01

Fig.1. video capture



Source Video: Capture From File

Prime Number 1: 7

Prime Number 2: 17

Enter "E": 5

Path: Users\VINEET\Desktop\Demo.d

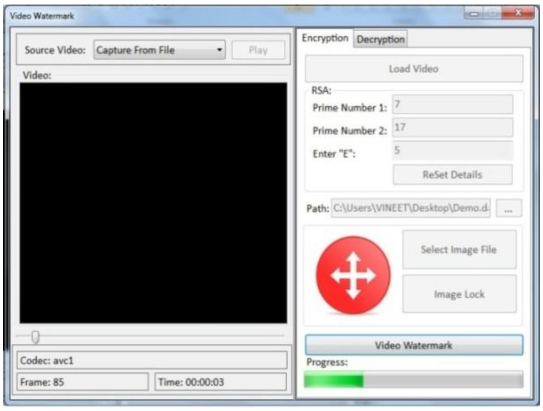
Image Locked Successfully

Codec: avc1

Frame: 85

Time: 00:00:03

Fig. 2. Lock the image



Source Video: Capture From File

Prime Number 1: 7

Prime Number 2: 17

Enter "E": 5

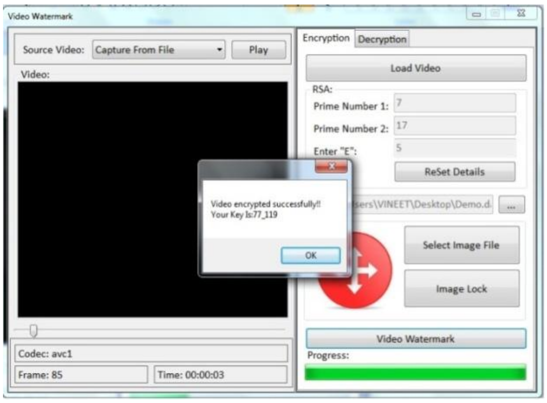
Path: C:\Users\VINEET\Desktop\Demo.d

Codec: avc1

Frame: 85

Time: 00:00:03

Fig. 3. Video watermark



Source Video: Capture From File

Prime Number 1: 7

Prime Number 2: 17

Enter "E": 5

Path: sers\VINEET\Desktop\Demo.d

Video encrypted successfully!!
Your Key Is:77_119

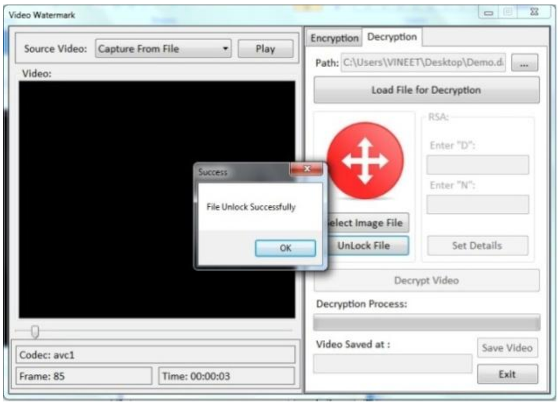
Codec: avc1

Frame: 85

Time: 00:00:03

Fig 4. Key generation

DOI: 10.15680/IJIRCCE.2015. 0310049


Video Watermark

Source Video: Capture From File

Path: C:\Users\VINEET\Desktop\Demo.d

Codec: avc1

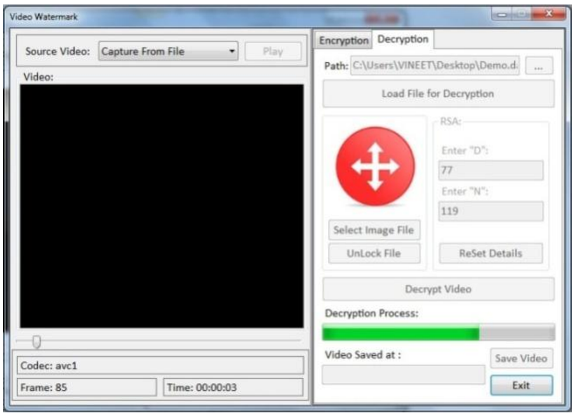
Frame: 85

Time: 00:00:03

Success

File Unlock Successfully

Fig. 5. Image File Unlock


Video Watermark

Source Video: Capture From File

Path: C:\Users\VINEET\Desktop\Demo.d

Enter "D": 77

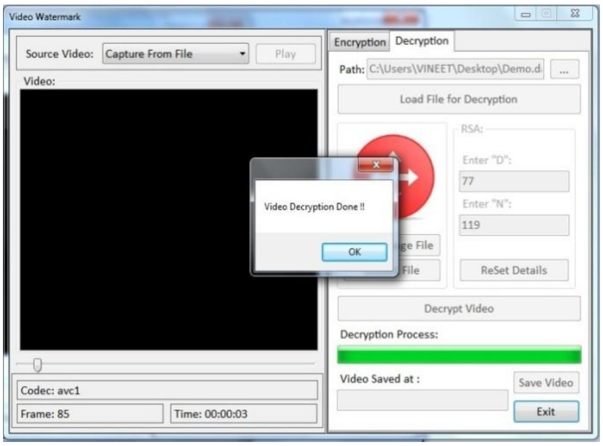
Enter "N": 119

Codec: avc1

Frame: 85

Time: 00:00:03

Fig 6. Decryption Process


Video Watermark

Source Video: Capture From File

Path: C:\Users\VINEET\Desktop\Demo.d

Enter "D": 77

Enter "N": 119

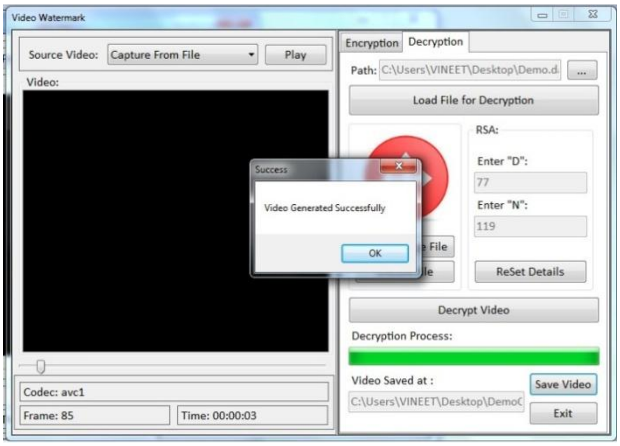
Codec: avc1

Frame: 85

Time: 00:00:03

Video Decryption Done !!

Fig. 7. Video Encryption Done


Video Watermark

Source Video: Capture From File

Path: C:\Users\VINEET\Desktop\Demo.d

Enter "D": 77

Enter "N": 119

Video Saved at : C:\Users\VINEET\Desktop\DemoC

Codec: avc1

Frame: 85

Time: 00:00:03

Success

Video Generated Successfully

Fig 8. Video Generated Successfully

VI. CONCLUSION AND FUTURE WORK

The results showed that the proposed algorithm performs better encryption with video watermarking to provide better security and authentication. The proposed video watermarking technique can be used in defense services, corporate world, education system, etc. it is a way to discourage illegal duplication of data by hiding information in data in such a way it is impossible to separate from data.

In future, we are encoding watermark into shares to authenticate shares as well. Which, we are taking one image and watermarking it with a secret image using DCT algorithm. After that we are going to make 2 shares from the watermarked image. One share will be stored into database and the other share will be given to the user with ID attached to it. This is the registration phase for the user. In authentication phase, user will bring the share given to him. This share will find the share stored in database by using the ID attached. Then by superimposing these two shares we will get watermarked image generated in registration phase. Then we will apply Inverse-DCT on watermarked image to check whether shares are valid or not.

REFERENCES

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

BIOGRAPHY

Ritesh Bagalkoti is a Professor of B.E Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University. He had done M.Tech in Computer Engineering**.**

Heena Sheikh is a B.E Student of Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India**.**

Ankita Pawar is a B.E Student of Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India**.**

Nikita Dhawade is a B.E Student of Computer Engineering, RMD Sinhgad School of Engineering, Savitribai Phule Pune University, India**.**