ISSN:0975-9646

Advanced Security using VCS and Watermarking

Minal Nerkar, Priya Talreja, Komal Pawar , Radha Gosavi, Devika Dhadphale

Department of Computer Engineering,

AISSMS IOIT Pune

***Abstract*— With the advent of internet, various online attacks has been increased. In this paper we are using visual cryptography algorithm for separating privileges. It is risky to upload confidential data directly on the cloud hence we are implementing video watermarking algorithm. Here combination of VCS and Video Watermarking gives enhanced security to our system and makes our system robust against attacks.**

***Keywords*— CAPTCHA, Watermark, LSB, SCD, DES**

I. INTRODUCTION

Online transactions are now a days become very common and there are various attacks present behind this. Thus the security in these cases should be very high and should not be easily tractable with implementation easiness. The concept of image processing and an improved visual cryptography is used. Visual Cryptography (VCS) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image.

Watermarking is a major image processing application used to authenticate user documents by embedding and hiding some authenticated piece of information behind an image, audio or the video file. Video watermarking involves embedding a secret information in the video. For example, copyright symbols or signatures are often used. The traditional watermarking approach tends to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer. Now a days more efficient and secured approach to perform watermarking is used. It is done by using invisible watermarking technique. Video watermarking is done by using Scene change detection technique which embeds different parts of a single watermark into different scenes of a video.

II. LIRETARURE SURVEY

Visual cryptography, an emerging cryptography technology, was proposed in 1994. It was called as secrete sharing scheme.

First the secrete image was encrypted and decrypted using human visual system. Secrete image is hidden in n different shares. Then these shares are stacked together to reveal the final secrete image. Any one share cannot reveal anything about secrete image. Hence, security level of the secrete image is increased when it is transmitted via internet. There are some schemes that take only binary images as secrete image. New cryptography schemes are also there that can process secrete colour images that are more complex.

Video watermarking embeds data in the video for the purpose of identification and copyright. Many digital watermarking schemes have been proposed for images and videos. It permits only authorized users to access encrypted digital data. Video watermarking introduces some issues which is not present in image watermarking. a robust video watermarking scheme is necessary.

III. MOTIVATION

Main limitation in today's online confidential data accessing system is there may be possibility that this data may be attacked by phishing websites therefore there comes need to identify whether website is phishing or not. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and
secure or not.

Existing video watermarking tools uses visible watermark. The main disadvantage of visible watermarking is that it destroys the video quality and watermark can be easily removed from video. In contrast, invisible watermarking is imperceptible to those viewing the video and the watermark is still present in the multimedia data even after various signal processing or transmission distortions.

IV. METHODOLOGY

A. Visual Cryptography

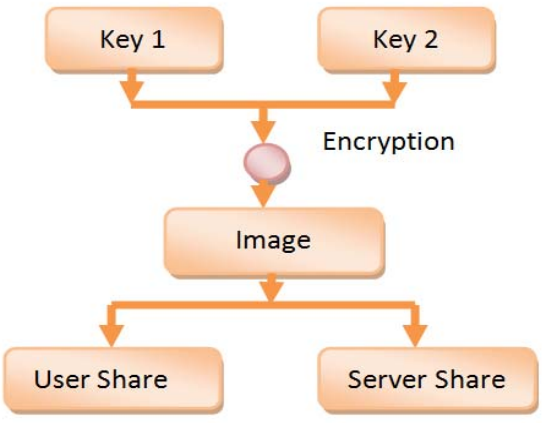


Fig. VCS

Steps:-

i. A(2,2) VCS can be described by the following 2*2 Boolean matrices.

$$M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

ii. A particular pixel P in the secret image is split into two sub pixels ,i.e. m=2 in each of the two shares.

iii. If the given pixel P is white, we use M0 to encrypt the pixel by setting the first row to s1 and setting the second row to s2, s1=(1,0) and s2=(1,0).

iv. The Hamming weight of the stacked version share V is H(V)=1, where V=s1+s2=(1,0).

v. If the given pixel P is black, we use M1 to encrypt the pixel by setting the first row to s1 and second row to s2, s1(1,0),s2(0,1).

vi. And the Hamming weight is H(V)=2, where V

vii. =s1+s2=(1,1).

viii. By stacking s1 and s2 together, a pixel P is interpreted by the visual system of the users as white if the Hamming weight H(V)=1 and as black if H(V)=2.

ix. By permuting the columns of M0 and M1, we obtain two collections of 2*2 Boolean matrices.

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}, C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

- To share a white pixel, we randomly choose one of the matrices in C0, and to share a black pixel, we randomly choose one of the matrices in C1.
- Note that permuting the column of M0 and M1 does not change the Hamming weight of the matrix. However, this procedure is required in order to satisfy the security condition.
- The algorithm for encrypting one pixel is introduced. This algorithm is to be applied for every pixel in the secret image to construct the two shares.
- Time Complexity- FOR VCS O(n).

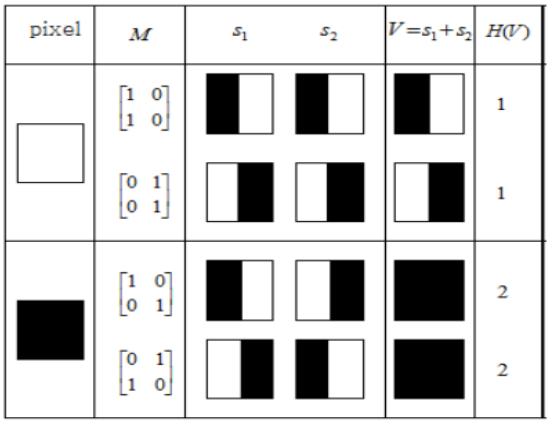


Fig. Encrypting algorithm of 2 by 2 VCS

B. Video Watermarking

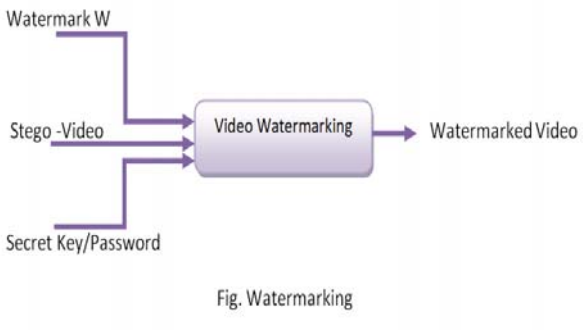
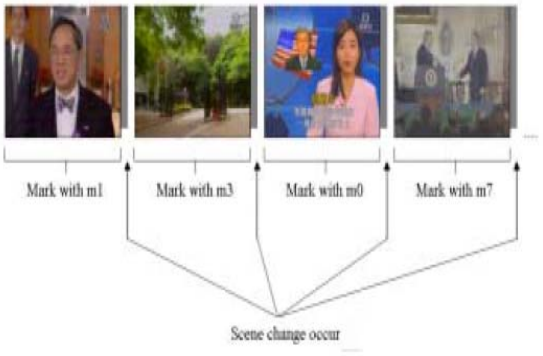


Fig. Watermarking

1. SCENE CHANGE DETECTION

- Input – Video
- Output - Video broken into frames



- Steps –

i. Take a video as input.

ii. Compute color histogram of each frame in video.

iii. For framecount =1 to number of frames -1

iv. Compare two consecutive frames based on their color histogram.

v. if distance between two consecutive frames fi and fj is greater than predefined threshold q then

1. scene is changed

else

2. scene is not changed.

- Time Complexity - O(n)
- Space Complexity - O(n

2. LEAST SIGNIFICANT BIT

- Input - Video frames and chunks of watermark
- Output - Encryption of watermark into frames
- Steps -

i. A few least significant bits are substituted within data to be hidden.

ii. The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.

iii. Let n LSBs be substituted in each pixel.

iv. Let d= decimal value of the pixel after the substitution.

v. d1 = decimal value of last n bits of the pixel.

vi. d2 = decimal value of n bits hidden in that pixel.
vii. If (d1_ d2) _ (2n)=2 then
no adjustment is made in that pixel.
Else
If(d1 <d2)
d = d - 2n:
If(d1 >d2)
d = d + 2n:

This d is converted to binary and written back to pixel.

- Time Complexity - O(n)

V. EXPREMENTAL RESULTS AND ANALYSIS.

A. Performance Measurement

The graph is robustness against fidelity which is an exponential graph which has two regions-

i. Achievable.
ii. Non-Achievable.

The upper region of exponential graph is **Non-Achievable** region and Lower region is **Achievable**.
This graph is raising and expanding at steady and rapid rate.

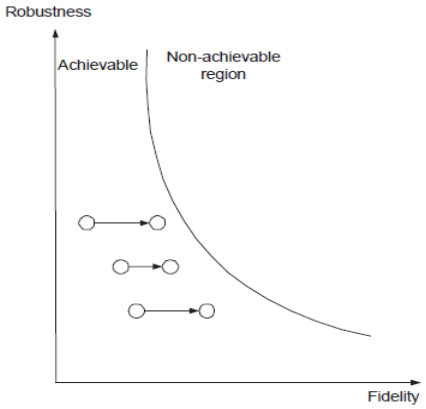


Fig. Performance Analysis.

B. FEASIBILITY CRITERIA

NP Complete
Non Deterministic Polynomial Complete. Problems for which there is a known solution. But the time required for generating the solution is not fixed. There is a guarantee that results will be generated in a finite time.
Our project is in NP complete.

Following are the reasons :-
1 Our project is divided into two parts. First part is login phase using visual cryptography scheme and second part is watermarking for upload and download data with video watermark. As we are providing security to both login phase and data, it should not be in NP hard or NP. Our Visual Cryptography algorithm will not go in infinite loop or it will not cause system to get stand by.

2 Same thing will happen for watermarking algorithms also. Output of this system will definitely come but time will not same for each output hence it is in NP complete.

C. RESULT ANALYSIS

a) Visual Cryptography
- Earlier the authentication method used was image CAPTCHA which was randomly generated by system without splitting image CAPTCHA.
- It was used just for checking whether user is human or robot.
- The technique we are using is VCS in which the CAPTCHA is split in two shares. One share is with user and other is with server.
- Hence, the security is enhanced as compared to earlier authentication techniques.

b) Video Watermarking
- Earlier visible watermarking techniques were used.
- Here in this paper we are using invisible watermarking technique.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

Various online attacks has been increased as boon of internet use. Attack is done and confidential data of user is fetched. We have implemented Visual Cryptography which is image based authentication which gives the user a secure login.

After successfully login of the system we can upload encrypted data on the system. The process of this comprehensive video watermarking scheme, including watermark preprocessing, video preprocessing, watermark embedding, and watermark detection, is described in detail. Various improvement approaches are also presented.

Experiments are conducted to demonstrate that our scheme is robust against attacks by frame dropping, frame averaging and statistical analysis. If we compare to the previous watermarking algorithmsis very much higher. Within certain range this watermarking algorithm is robust to the video compression and video frames attacks.

B. Future Scope

i) This system can be used in cloud computing which can enhance its security.
ii) As the generated CAPTCHA is divided into two shares one with user and other with server access two simultaneously will be difficult for the attacker. So the system can used in antiphishing website.
iii) As both the watermarking and VisualCryptography is used. The system can be used in Army for security purpose like sending and receiving encrypted data. and preserving Government confidential data.

REFERENCES

[1] Akash Mehara, Emon Vuess ,Enhanced Security in Cloud Computing(IEEE 2014)
[2] Divya James, Mintu Philip, A Novel Anti Phishing framework based on Visual Cryptography(IEEE 2014).
[3] Video Watermarking for Copyright protection using Scene Change Detection Algorithm(White Paper).
[4] Pik Wah Chan, Student Member, IEEE, Michael R. Lyu, Fellow, IEEE, and Ronald T. Chin, A Novel Scheme for Hybrid Digital Video Watermarking: Approach, Evaluation and Experimentation.
[5] Hamid Shojanazeri, Wan Azizum Wan Adnam, Sharifah Mumtadzah SyedAhmed, Video Watermarking Techniques for Copyright Protection and Content Authentication(International Journal of CIS IMA 2013).
[6] Rini T Paul, Review of Robust Video Watermarking Techniques(NCCSE 2011).
[7] Gopika V Mane, G G Chiddarwar, Review Paper on Video Watermarking Techniques(International Journal of Scientific Research Publication,2013,April 2013).