ISSN 2395-1621

Cryptography using Captcha Authentication

[#1]Akshaykumar Digrase, [#2]Abhinav Chavan, [#3]Sushant, [#4]Prof. Navdeep Bagga

[1]digraseakshaykumar86@gmail.com

[#123]Department of Computer Engineering
[#4]Prof. Department of Computer Engineering

G. H. Raisoni Institute of Engineering and Management, Pune.

ABSTRACT

With the advent of internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal con dential information such as passwords, credit card information from unsuspecting victims for identity theft, nancial gain and other fraudulent activities. We are using visual cryptography algorithm for separating privileges. Due to rapid growth of internet and multimedia systems now it is easier to copyright the multimedia documents like audio, video, text, images etc. Video piracy has become an increasing problem particularly with the proliferation of media sharing through advancement of Internet services. Since digital video can be easily and perfectly duplicated and illegally distorted, appropriate schemes are needed to protect the rights of content owners or the integrity of the surveillance video les. Now days there are many techniques available for providing security to multimedia documents. Video watermarking is an important emerging technique for these issues. In our sys-tem we propose scene change detection (SCD) watermarking algorithm which is the most convenient and efficient method for copyright protection of video. This method is more robust to withstand with different types of video attacks like frame dropping, lossy compression. Here combination of both the Schemes is implemented so as to give enhanced security to the system. This makes our system robust against all type of attacks.

ARTICLE INFO

Article History

Received: 28th May 2016

Received in revised form :

28th May 2016

Accepted: 1st June 2016

Published online :

2nd June 2016

Keywords: **SCD, Watermarking, Captcha, Hidden Message.**

I. INTRODUCTION

OVERVIEW

Visual Cryptography is a new Cryptography technique which is used to secure the images. In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the bi-level or binary images or monochrome images. Later it was advanced to suit for the colour Images means Gray Images and RGB/CMY Images.

The protection and illegal redistribution of digital media has become an important issue in the digital era. This is due to the popularity and accessibility of the Internet now a days by people. This results in recording, editing and replication of multimedia contents. Video watermarking can be used to protect data against illegal manipulations and distributions. This technique provides a robust solution to the problem of intellectual property rights for online contents.

BRIEF DESCRIPTION

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 le. 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. PROBLEM STATEMENT

Online transactions are now 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 le. 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.

III. PROPOSED SYSTEM

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other con dential information from the phishing websites. We also propose the idea of embedding different parts of a single watermark into di erent scenes of a video. We then analyze the strengths of different watermarking schemes, and apply a hybrid approach to form a super watermarking scheme that can resist most of the attacks. For implementing Watermarking Technique we are using SCD, LSB, Split ,DES algorithms.

The proposed approach can be divided into three phases:

A. Registration Phase

In the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later veri cation during login phase. The image captcha is also stored in the actual database of any con dential website as con dential data. After the registration, the user can change the key string when it is needed. Registration process is depicted in figure Registration phase.

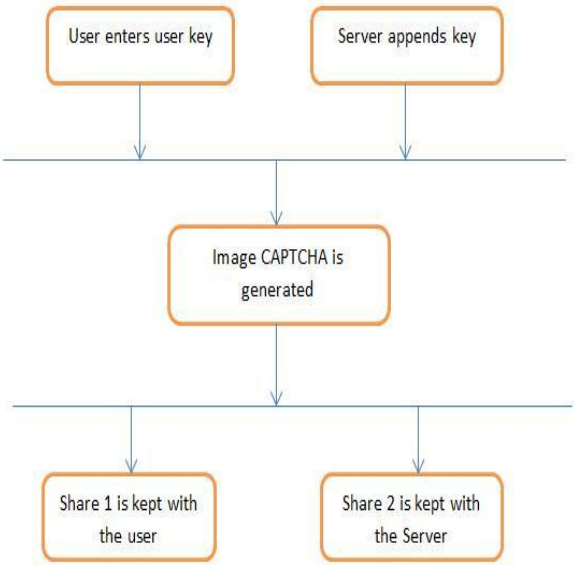


Fig 1. Registration Phase

B. Login Phase

When the user logs in by entering his con dential information for using his account, then rst the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not. This phase is depicted in Figure login phase.

C. Watermarking Phase

We propose the idea of embedding different parts of a single watermark into different scenes of a video. We then analyze the strengths of different watermarking schemes, and apply a hybrid approach to form a super watermarking scheme that can resist most of the attacks.

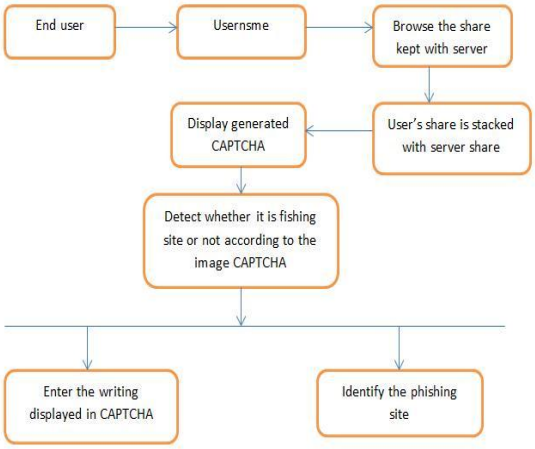
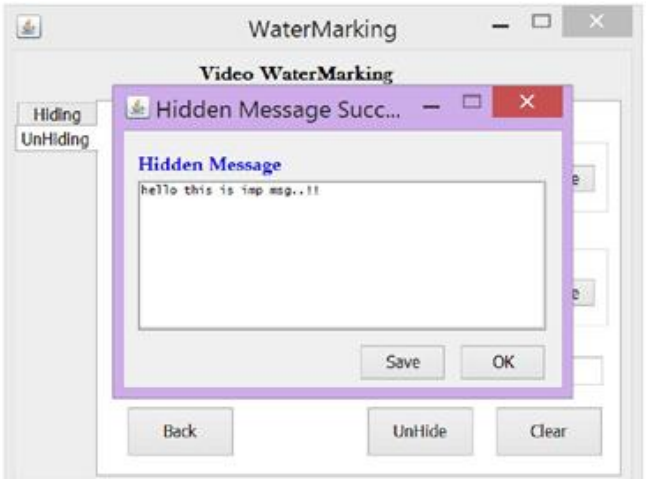


Fig 2. Login Phase

Figure 2.4: Watermarking Phase

IV. RESULT



V. CONCLUSION

With the advent of internet, various online attacks has been increased. . Here an image based authentication using Visual Cryptography is implemented. 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.

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 Detec-tion 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 Water-marking: Approach, Evaluation and Experimentation.

5. Hamid Shojanazeri, Wan Azizum Wan Adnam, Sharifah Mumtadzah Syed Ahmed, 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 Scienti c Research Publication,2013,April 2013) .

