International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), 4 Issue-5, November 2015

Secured Password Verification Captcha using Visual Cryptography

Aparna Raut, Kiran Sukal, Anushree Khedekar, Monika Mohimkar

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 confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. We are using visual cryptography algorithm for separating privileges. The use of visual cryptography is explored to preserve the privacy of an image CAPTCHA by decomposing the original image CAPTCHA into two shares (known as sheets) that are stored in separate database servers(one with user and one with server such that the original image CAPTCHA can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image CAPTCHA. Once the original image CAPTCHA is revealed to the user it can be used as the password. of attacks.***

Index Terms— Visual Cryptography, SCD, DES, LSB

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanisms should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness .The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) 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. Nowadays more efficient and secured approach to perform watermarking is used. It is done by using sub image classification, i.e. selected frames only will contain a fractional number of total bits from the watermark image. Video watermarking is done by block based Scene change detection technique which embeds different parts of a single watermark into different scenes of a video.

Revised Manuscript Received on 30 November 2015.
* Correspondence Author
Miss. Aparna Ankush Raut, Department of Computer Engineering, SPPU, Modern Education Society's College of Engineering, Pune, India.
Miss. Kiran Sukal, Department of Computer Engineering, SPPU, Modern Education Society's College of Engineering, Pune, India.
Miss. Anushree Khedekar, Department of Computer Engineering, SPPU, Modern Education Society's College of Engineering, Pune, India,.
Miss. Monika Mohimkar, Department of Computer Engineering, SPPU, Modern Education Society's College of Engineering, Pune, India.

II. SYSTEM ARCHITECTURE

System design provides the understanding and procedural details necessary for implementing the system recommended in the system study.

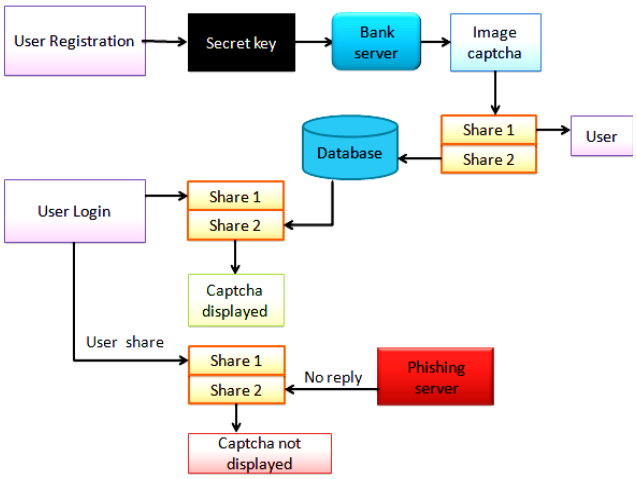

Fig. 2. 1. System Architecture

III. PROPOSED METHODOLOGY

Watermarking Technique we are using SCD, LSB, Split ,DES algorithms. The proposed approach can be divided into three phases: [2]

A. Registration Phase

In the registration phase, a key string(password) is asked from the user at the time of registration for the s 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.[2]

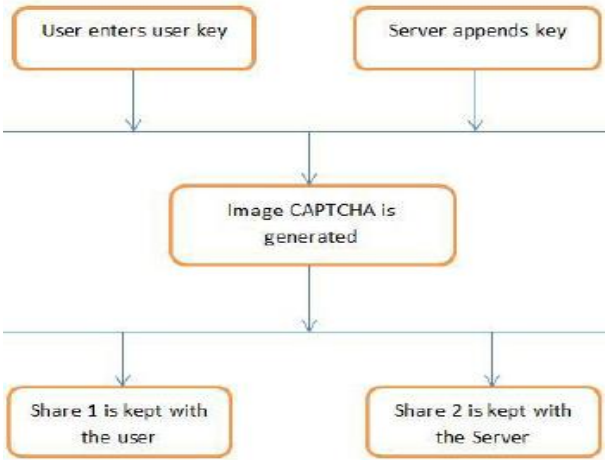

Fig.3.1.Registration Phase

B. Login Phase

In the login phase the user is asked to enter his share which is kept with him. 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.[2]

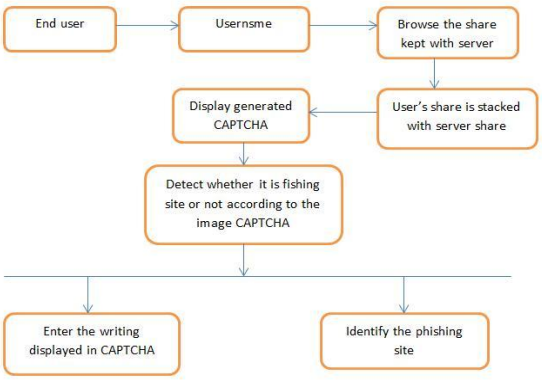

Fig.3.2.Log In Phase

C. Watermarking Phase

Here in this technique we are going to use 4 different schemes:

1) SCD(Scene change detection algorithm)
2) LSB(Least significant bitalgorithm)
3) DES(Data Encryption Standard). [5]

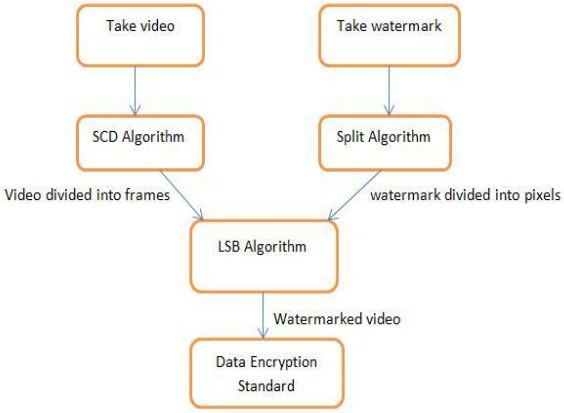

Fig 3.3. Watermarking Phase

IV. PROJECT SCOPE

Using visual cryptography the user will be able to login securely. Invalid User will not be able to login on the site. Personal and con dential information will be secure. In this, the user will be waiting for a period of time to receive the reconstructed CAPTCHA. If the user does not receive correct CAPTCHA or wrong CAPTCHA then he will not be able to login. After login user will be able to encrypt the data in the video so as to keep the data in secure form.

V. CONCLUSION

In this paper we concluded that 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.

ACKNOWLEDGEMENT

We thereby thank our college MES College of Engineering (MESCOE), Pune for the motivation. Also we would like to thank our guide Mrs. Shraddha. R. Khonde for her active support.

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 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 Scientific Research Publication,2013,April 2013)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)