

A Hash Based Visual Cryptography Anti-Phishing Scheme

Divya Anwesh Sahu
M Tech (Data Analytics), Dept. of CA
National Institute of Technology
Tiruchirapalli, Tamil Nadu
dibyaanwesh@gmail.com

Abstract— This paper describes the implementation of an anti-phishing framework with the help of visual cryptography. In this method we test the server that is under test through image-based authentication which is secured and safe. A secret random image that is to be transmitted is encoded into two shares, called client share and server share. It involves the client and server storing their respective shares and then overlapping them to produce the original secret image thus authenticating the required side.

Index Terms — Visual Cryptography; key share; hash; Phishing; user share

I. INTRODUCTION

In this modern world so much of what we do is being carried out online, starting from booking movie tickets to businesses and bank transactions. If its not done yet then methods are being searched and researched to make them happen. We are currently walking on a thin thread between convenience and security. On one side convenience is expected from services and products like a feature whereas on the other side security is an essential commodity without which the world would break.

Cybercrime has become increasingly powerful and dangerous tool for criminal to steal and extort money or information on the target. One of the most popular and successful attacks is phishing. It is a type of online theft that aims at stealing credit card information, bank credentials, passwords, etc. by pretending to be a

trustworthy entity (masquerading) during an online transaction or by email. It is considered as a mixture of social engineering practices and technical deceit. In phishing the criminal doesn't directly hack into the user's electronic device but tries to convince or persuade them into doing a series of action that might lead to them gaining confidential information. Phishing attacks can be many types attempted through various mediums for example: whaling, tab nabbing, rouge Wi-Fi, spear phishing, clone phishing, link manipulation, etc.

The most widely used communication channels are through web pages, e-mails and instant messaging and the most successful among these is e-mails. In this project we will concentrate on web link based phishing attempts where the URL of original websites are cleverly modified by hiding misspellings and affixes, and then the clicked web pages are also so accurately copied that they look like the real ones which is then wrongly interpreted by the user as correct web pages. Thus the user is tricked into giving confidential information to the phisher.

II. VISUAL CRYPTOGRAPHY

Visual cryptography is a scheme to hide a secret image using any number of shadow image called shares. The secret image should be a grayscale image or if color we need to convert it into grayscale. When we break the image into shares they alone on themselves don't look like anything but when they are layered on top of another they return back the original image. This particular algorithm used in this project uses the patterns showed in figure 1. If the same patterns are layered on top of another they return the same pattern and if the opposite patterns are used, they give a black image. The trick in the algorithm is the way the shares are created.

We simply use the data from the hidden image and use the concept of sampling distribution of mean.













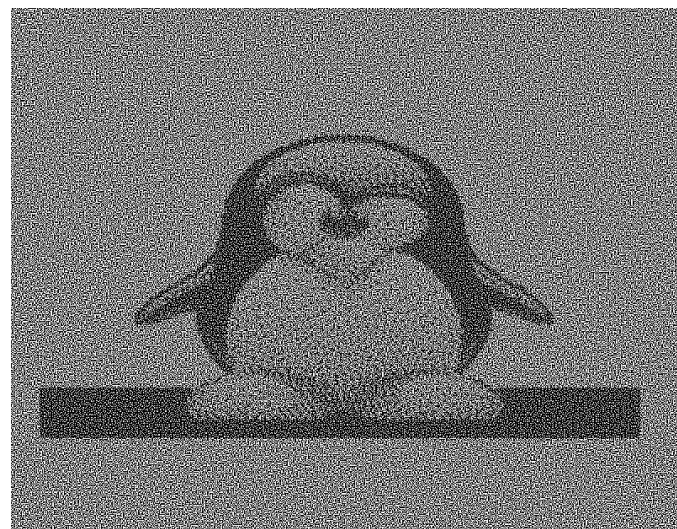
pixel		share #1	share #2	superposition of the two shares
	$p = .5$			
	$p = .5$			
	$p = .5$			
	$p = .5$			

Fig 1: Figure that shows how each pixel is divided into 4 parts and then the sub-part's colour arrangement is changed to either allow partial amount of light to pass or nothing at all.

In our implementation we perform a slightly modified visual cryptographic scheme in which the picture to be hidden is divided into shares in such a way that two totally different seemingly innocent images are displayed as a partially blurred images. But when we combine them they reveal the original to-be-hidden image. We can see them working in figure 2.



Share 1



Share 2



Fig 2: Dummy image being embedded on a share

Fig 3: Working of Visual Cryptography

Text-based passwords are the most popular form of authentication today and with that attacks on them have become common now-a-days. Therefore new methods and schemes are under research and development. One such Method is Visual cryptography. We use hashes of shares and store them in database with username and password. Since it is impossible to get the share back from hash it provides us a secure method to store data. This scheme provides us a secure way to authenticate user and servers under contact.

III. APPROACH

The major entities involved the current scheme are client, Trusted Server (TS) and Server under Test (SUT). A secured methodology is proposed to verify the authenticity of the server using the concept of visual cryptography. This system uses an image-based authentication by decomposing a random image into two shares in a particular session. The trusted-server helps the client in identifying the genuineness of the

server-under-test by performing decryption of the shares. Then the server-under-test is finally determined as legitimate or not before the client accesses the server.

Client

A Client is a user in an organization or a single user who wishes to access the trusted server and Server under Test (SUT) for accessing the information over internet. The client accesses the Server under Test through the Trusted Server. In this paper we propose a verification of the identity of the SUT also to prevent the phishing attacks. The frequently accessed SUT's are authenticated by the trusted server and authentication of client and trusted server is also done.

The client has to register to the trusted server and authentication between both these parties is done with the assistance of visual cryptographic methodology where an image is selected and split into shares and shared by both the parties. If the original image is overlapped and the result is the appropriate image then both the parties are authenticated. The same functionalities are explained in detail below:

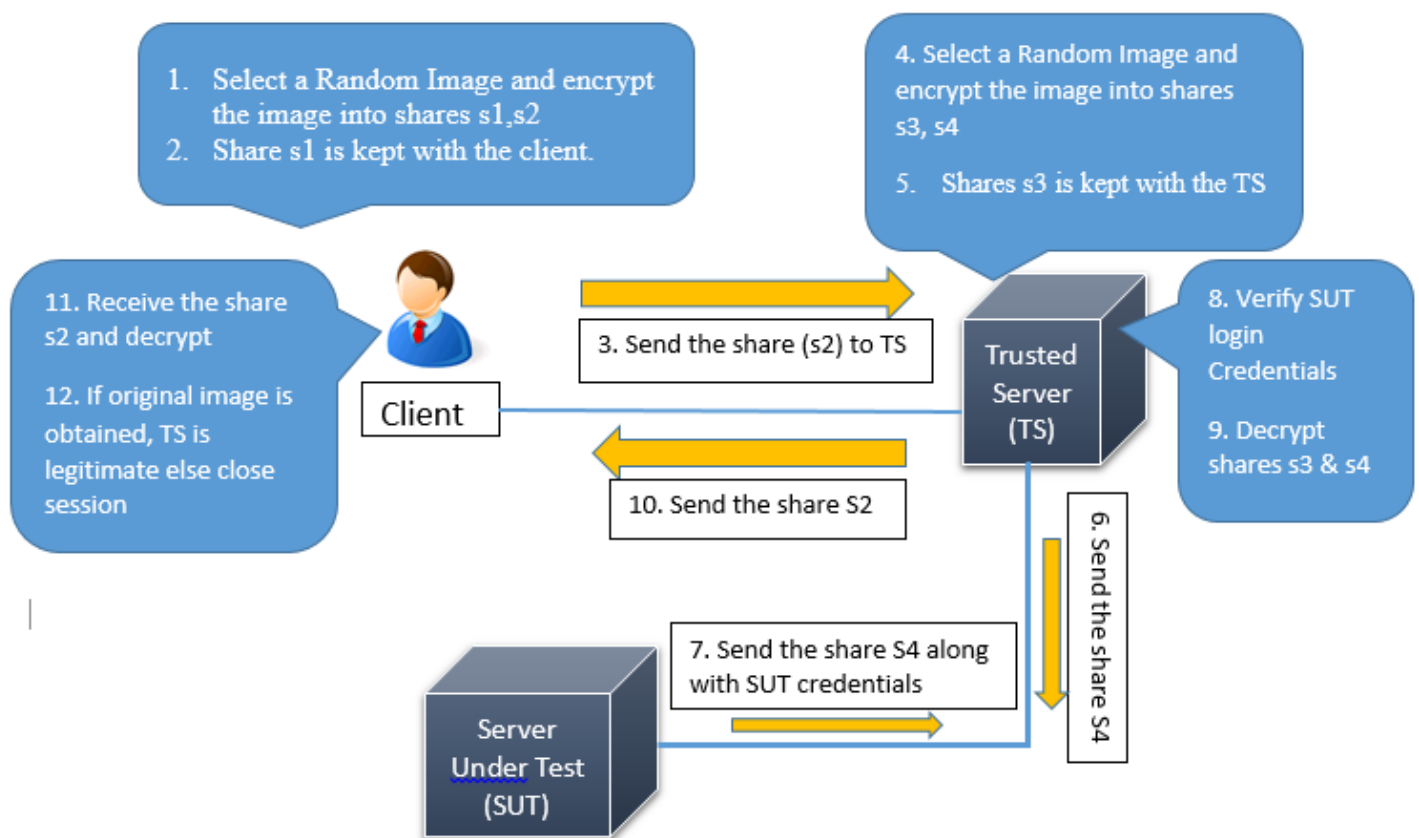


Fig.4 Proposed System Model

Client's functions:

(i) Registration to the Trusted Server (TS)

- Select a Random image.
- Encrypt the image into two shares (S1, S2).
- Distribute the share (S2) to TS.

(ii) Access

- Receive the share S2 from trusted-server after login.
- Perform decryption with S1 hosted with the client and the received share S2.
- Verify original image with the final decrypted image.
- If there is a match the TS is authenticated and the further process continues or else the request is turned out as Phishing attack.

This process of authentication prevents the phishing of Trusted server.

Trusted-Server:

Similar to that of the client and trusted server authentication, we name the shares used here as S3 and S4. The authentication at this point assures that the SUT is not being phished. The detailed process done by the Trusted Server is listed below:

(i) Registration

- Register the frequently accessed local servers for surfing. (Process is same as that of client-TS registration)

- Random image selection.
- Encrypt the image into two shares (S3, S4).
- Distribute the share (S4) to Server Under Test (SUT) and retain S3

(ii) Access

- Receive server-under-test credentials and verify.
- Receive share S4 from server-under-test.
- Decrypt S4 share with its own share S3.
- Verify original image with the decrypted image.
- If there is a match the SUT is authenticated or else it is understood that an attack has occurred.

This process prevents the phishing of Server Under Test.

Server-Under-Test

- Receive share S4 from TS during registration.
- Send its credentials and the received share to trusted-server during verification process by TS.

The client logs into the server with his username and password (these credentials were obtained during client's registration with the server). After a successful login, the client selects a random image and divides it into two shares (encryption). Share-1 is stored with the client in his database, share-2 is sent to the trusted-server. The Trusted server registers frequently accessed server for surfing. These servers are referred as server-under-test in this paper. The registration process of SUT – TS is similar to that of Client – TS. The TS authenticates

Registration Phase

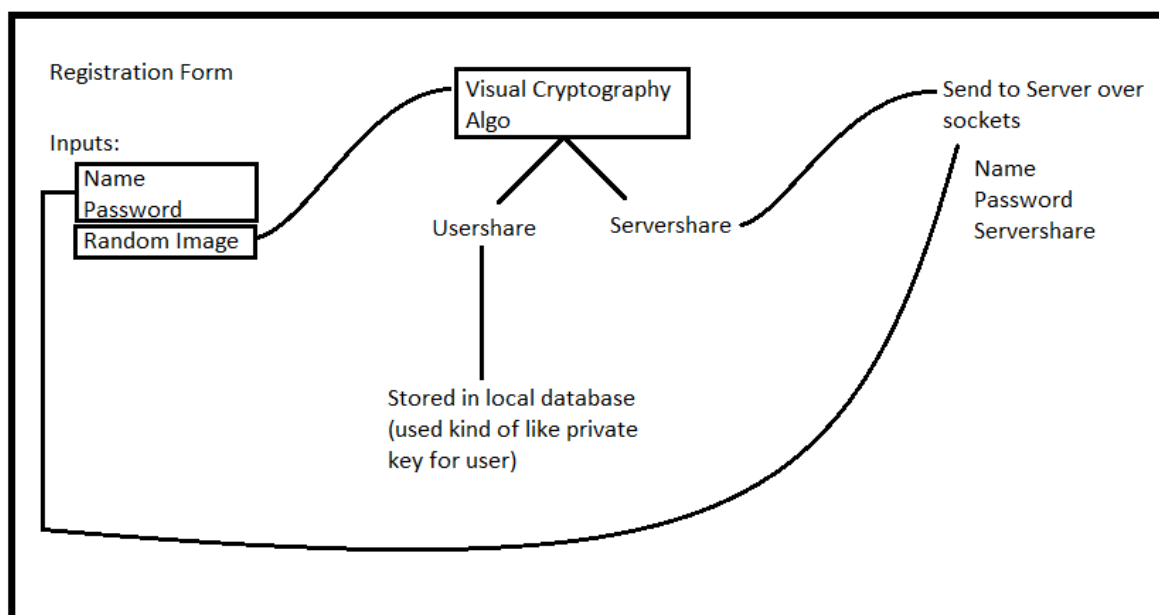


Fig. 5 The Registration Phase

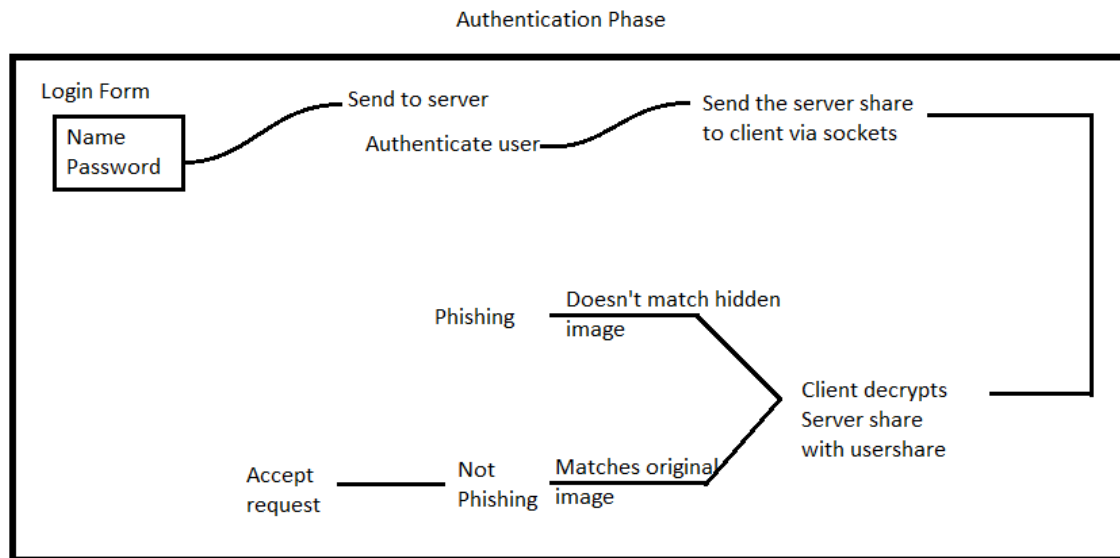


Fig. 6 The Authentication Phase

clients and client authenticates TS to assure that TS is not phished. Similarly SUT sends its share along with its credentials to the trusted-server for verification of its genuineness. The trusted-server verifies the credentials to check whether the server-under-test has been previously registered to it. If these credentials are accurate trusted server decrypts share-4 and share-3 and thus authenticates the SUT that it is not phished.

IV. NOVELTY

1. This implementation uses image based authentication.
2. We use hashes rather than sensitive data to store the information.
3. This method authenticates both the trusted servers and the server under test as both can be used as points of attack.

V. CONCLUSIONS

The proposed methodology helps to be secure online phishing attacks. This methodology assures more security as the visual cryptography technique is applied on a random image selected for every new server-under-test. All the three entities (Trusted-Server, client, Server-Under-Test) are authenticated and assure that every entity is original. This assures that all the entities are protected from being disguised. Performing decryption

at two different stages to obtain the final image assures more security. This proposed methodology safeguards the users from phishing attacks. When there are multiple server-under-test's for verification, there is load on the trusted-server for checking credentials of too many server-under-tests. This is a major limitation of this proposed technology. This can be overcome by continuing the session once an SUT is authenticated. Authentication is done only when a new session is to be started.

VI. REFERENCES

- Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar and Prof. S. Baj, (2014), An Enhanced Anti-Phishing Framework Based on Visual Cryptography, International Journal of Emerging Research in Management & Technology, Vol. 3, Issue-3.
- Anushree Suklabaidya and G. Sahoo, (2013), Visual Cryptographic Applications, International Journal on Computer Science and Engineering, Vol. 5 No. 06.
- Y.Yesu Jyothi, D. Srinivas and K. Govindaraju, (2013), The Secured Anti-Phishing approach using image based validation, International Journal of Research in Computer and Communication Technology, Vol. 2, Issue 9.
- A.Angel Freeda, M.Sindhuja and K.Sujitha, (2013), Image Captcha Based Authentication Using Visual Cryptography. International Journal of Research in Engineering & Advanced

Technology, Vol. 1, Issue 2.

B.Padhmavathi, P.Nirmal Kumar and M.A.Dorai Rangaswamy, (2010), A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography using Image Processing. International Journal on Signal and Image Processing, Vol. 1, No.3.

B. Borchert, (2007), Segment Based Visual Cryptography, WSI Press, Germany, 2007.

Sonal Wange, (2013), A Visual Cryptography to secure Biometric Database: A Review, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue-11.

Shital B.Pawar, Prof.NM.Shahana, (2013), Visual Secret Sharing Using Visual Cryptography, International Journal of Engineering Research Vol. 3, Issue 1.

G Lakshmeeswari* and Shubham Goel, (2016), Anti-Phishing Frame-Work applying Visual Cryptography Mechanism, Vol.6, Issue1.

Gonela Shiva, CH. Samson, (2017), A Hash Based Visual Cryptography Scheme for Image Authentication, Volume: 2 Issue: 8