International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

# A novel Mutual Authentication algorithm using visual cryptography with novel visual cryptographic schemes

**Daisy Das[1], Amarjyoti Pathak[2]**

[1]*M.tech, Computer Science And Engineering Department,Girijananda Institute Of Management And Technology,Guwahati, India*
[2]*Assistant professor,Computer Science And Engineering Department,Girijananda Institute Of Management And Technology,Guwahati, India*

---

**Abstract -** *We proposed a mutual authentication scheme using visual cryptography. Traditionally text-based username and passwords are used to authenticate a user to any online service. Authentication using passwords are old as well as less reliable regarding security. Passwords if kept too simple is prone to identity theft and if too complex difficult to remember them. Complex passwords require sophisticated encryption and decryption algorithms. This paper proposes a method of providing mutual authentication security by using Visual Cryptography It offers a means of providing security by using Visual Cryptography. This scheme provides mutual Authentication security without third party intervention where the client can authenticate the server and vice versa.Mutual Authentication is a significant factor in E-banking or E-commerce applications to counter cyber attacks. Visual Cryptography is applied to the security images registered by a user where the server generate shares and distribute the user via mail initially of one image. The second image share is generated randomly and circulated to the user during login as session password. The user uploads its initially received registered share to validate the server. The server compares the hash of the user usual password and security image random share to authenticate the user. This scheme can provide both user authentication and phishing attack generating mutual authentication between parties. Since the shares are created, which are not useful for the internal hackers. .The proposed mutual authentication scheme creates individual shares of user-uploaded images and uses these shares to login into the system. The method improves security measure between existing authentication model.*

***Key-words—visual cryptography; mutual authentication; shares; keyless; image; computational complexity, accuracy; secrecy; thresholding; algorithm***

## 1. INTRODUCTION

With growing popularity of the internet, most applications are insecure. People often use facilities provided by institutions for online transactions. But for layman there are a lot of security issues occurring during an online transaction; some major security threats are phishing, password reuse, password theft, brute force & dictionary attacks .However, due to the increasing rate of malware, currently, detection of fake website or fake user, hacker has become a severe problem for the users. As a result, it is not possible to be sure whether we are using a authenticated server or not and not been trapped. These give rise to mutual authentication so as both the user and server authenticate each other. The primary motive is to have an authentication algorithm that is effective, not easily tractable & with implementation easiness. In this paper, a secured mutual authentication scheme is proposed where in place of using conventional encryption and decryption techniques we went for visual cryptography techniques. The traditional cryptographic methods are sophisticated as well as require high computation and lot of decryption time. In addition to that, these methods are prone to many cyber security attacks. Visual cryptography was first proposed by Naor and Shamir[1] in 1994 based on the concept of secret-sharing. It divides an image into n shares where none of the individual shares reveal any information. The decrypted message is obtained by overlapping of the secret shares.

## 2. LITERATURE REVIEW

Many different methods have been designed and developed employed for attaining security about mutual authentication. The current security measure is having an SSL/TLS connection and a certificate issued by competent authority. The vulnerability that lies is that the validation of the license is the work of the browser and not the SSL/TLS specifications, it merely passes the certificate to the browser. At such fake certificate, attacks can take place[2].Moreover, users pay less attention to read the URL.**WIKID[3]** is a JSP application. WiKID is an existing software available for two-factor authentication for a specific price. The user login to their targeted site by starting their WIKID client and entering the pin. The PIN is then encrypted by the server's public key and sent to the server. If the PIN is found to be valid, the encryption valid and the account active, a package of the OTP, the target site URL and a hash of the target site's SSL certificate are sent back to the token client. The token client then goes out over the user's internet connection to the requested site URL and gets the SSL certificate, it then hashes it and compares the produced hash to validated certificate hash. If the two hashes match, the token client presents the

OTP and platforms) launches the default browser to the site for the user[3]. TrustBar[4], is a browser extension for identifying trusted sites. Using trust bar an user can assign a name or a logo to a secure site using TrustBar when the browser shows that secure site; otherwise, TrustBar presents the certified site's owner name and the name/logo of the Certificate Authority (CA) who identified the owner. Some of these ideas have already been adopted by application browsers, following the work. They describe usability experiments, which measure, and prove the effectiveness, of TrustBar's improved security and identification indicators[4].

## 3. VISUAL CRYPTOGRAPHY

The main aim of visual cryptography is image splitting where an image is split into n individual shares, and each share does not produce any information individually only when the shares are joined or overlapped they create the necessary information. The main demerit of visual cryptography is their poor reproducibility of original data.

## 4. PROPOSED METHOD

The proposed system offers a two-way mutual authentication algorithm which could be used to strengthen the existing authentication system of any organization minimizing the risk of false authentication and phishing sites. The system uses two user registered images which and traditional user defined password.

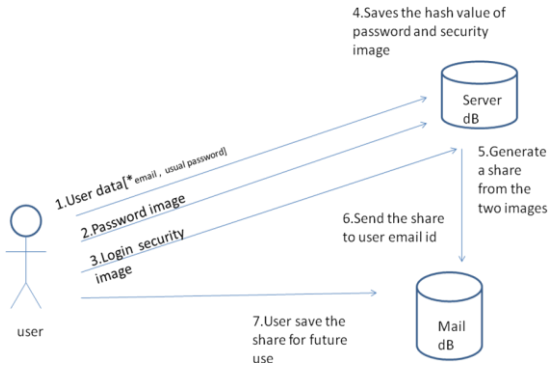


**Fig- 1: Registration phase**

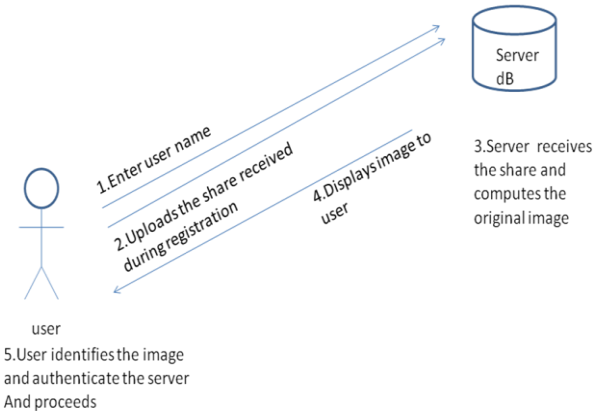


**Fig- 2: Login Phase-Server Authentication**

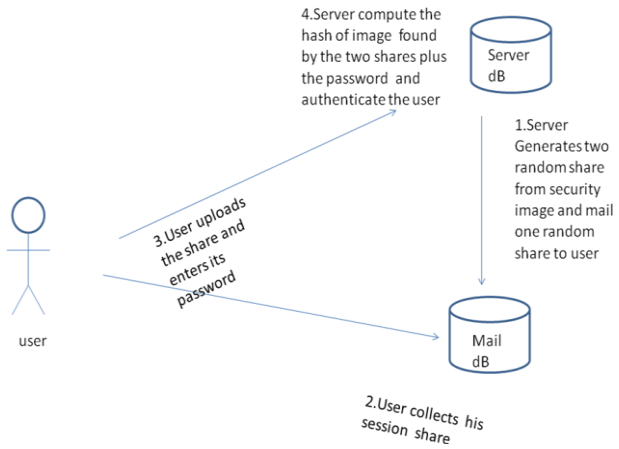


**Fig -3: Login Phase Server Authentication**

### 4.1 PROPOSED ALGORITHM

The proposed algorithm works in two phase.

1.Registration

2.Login

### 4.1.1 REGISTRATION PHASE

***Step 1:*** In the proposed algorithm we use the concept of visual cryptography where a user needs to register using two images (*security and password*), usual user data and traditional user password during the registration phase in the server.

***Step2:*** The server calculates the hash of the traditional password and password image provided by the user and stores it in the DB with other user credentials.

***Step3:*** The server generates a share with the two images and mails it to the user using user's registered mail id.

***Step4:*** The user collects its registered share from its email id and saves it for future use.

### 4.1.2 LOGIN PHASE

### AUTHENTICATING SERVER

***Step1:*** The user logs into the server.

***Step2:*** First it checks whether the given website is authenticated or not.

***Step3:*** It uploads its user share received during the registration phase.

***Step4:*** If the user's security image is reconstructed in the user side than the server is authenticated.

## AUTHENTICATING USER

***Step1:*** The server generates two random session share of users password image and mails one share to users registered mail id and keeps one with itself.

***Step2:*** The user collects its session share and upload it to the server

***Step3:*** The server reconstructs an image from uploaded users random share and server share

***Step4:*** The server then obtains a hash of user traditional password and image obtained in the previous step

***Step5:*** If the hash match with users registered hash value than the user is authenticated.

It gives a higher level of security as no two shares could produce the same image and at the same time set both user and server authentication. It also prevents against traditional password theft or reproducing attack as each time a new share of the same image is generated.

## 5. IMPLEMENTATION DETAILS

The system was implemented in JSP, HTML, and JAVA by using the thresholding /RGB plane slicing/image subtraction /RKO[5]technique to generate the user share, random share and server shares. The images were stored in the mySQL database, and the user share and random shares were sent to the user using Hmailserver which was obtained by Microsoft Outlook email client. The user's registered image constructed by the user share and DB image was displayed during the server validation phase so as to authenticate the server Secondly when the user needs to be authenticated it is verified by performing a hash of user password with random share uploaded by the user during login phase. The communication between client and server was through https connection.

## 6.EXPERIMENTAL RESULTS

**Color Image**

The method was implemented(*shown only for threshold , working with other methods are similar only the algorithm used to generate shares are different*) using two color image in Eclipse showed in Fig 4.

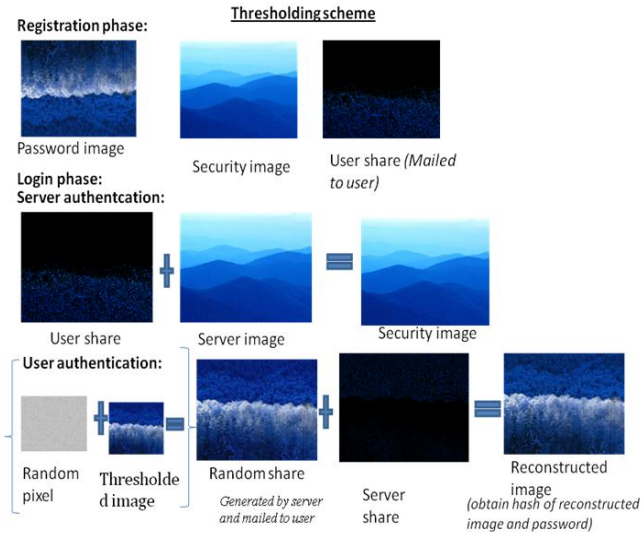


**Fig -4: Experimental output**

## 7. RESULTS AND DISCUSSIONS

In this proposed method the recovered image is a replica of the original image as no information is lost during the operations. The results were validated using the hash of the password and recovered image, and it was same as in DB obtained during the registration process

**Table 1 Comparison on existing scheme**

| Features | Proposed algorithm | Needham | Kerberos | skid |
|---|---|---|---|---|
| Third party | N | Y | Y | N |
| Mutual authentication | Y | Y | Y | Y |
| Man in middle attack | Y | N | N | Y |
| Session key | Y | Y | Y | N |
| Timestamp | N | N | Y | N |
| Replay attack | N | Y | N | Y(IF KEY KNOWN) |

## 3. CONCLUSIONS

In this project, a novel mutual authentication scheme is presented using Visual Cryptography technique. It is a traditional VCS and the conventional image encryption schemes. Visual Cryptography is applied to the security images registered by the user where the server generate shares and distribute the user via mail initially of one image.

The second image share is generated randomly and distributed to the user during login as session password. The user uploads its initially received registered share to validate the server. The server compares the hash of the user usual password and security image random share to validate the user. The technique adds security against malicious sites and unauthorized users. The proposed algorithm has the following merits.

1.Thus by the proposed algorithm, we achieve a mutual authentication using VC without any third party intervention.

2.It is not affected by mobile devices physical presence or network.

3.No complex computation needed by the user since normal vision can decode images.

4.The server can have a profile image of the user and its signature which is necessary for banks database, so no extra storage required.

5.Phishing is prevented for layman user.6.Password theft or reuse is prevented since each time a random share is used.

7.A third party cannot have user password, random share, and initial share at the same time.8.Brute force, replay attacks, a man in middle attacks are prevented.9.Finally, it is not easily traceable and achieved with implementation easiness.

The proposed scheme is suited for entity authentication based application where authentication can be done by overlapping the shares over one another to reveal the secret information. If the secret image matches the original image, then access is granted else denied.

## REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography," Advances in cryptology– Eurocrypt, pp 1-12,1995.

[2]http://u.cs.biu.ac.il/~herzbea/Papers/ecommerce/spoofing.htm

[3]https://www.howtoforge.com/prevent_phishing_with_mu

tual_authentication#prevent-phishing-with-mutualauthentication

[4] http://eprint.iacr.org/2004/155.

[5] Ms. Moushmee Kuri, Dr. Tanuja Sarode, "RKO Technique for Color Visual Cryptography", in: IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 89-93