

Secured Authentication for Banking Services using Visual Cryptography

G. Mohini¹ & M. Chandra Sekhar²

¹PG Scholar, Department of CSE, MVR College of Engineering and Technology, Paritala. Krishna District, A.P, India.

²Assistant Professor, Department of CSE, MVR College of Engineering and Technology, Paritala. Krishna District, A.P, India.

Abstract:

Now a day's authentication plays a very important role in banking services. But, because of hacking it is not safe to depend on text passwords and graphical image passwords. Services providing system need to be more secure and reliable because each and every task performed is related to customer's money and customer's confidential data. Especially authentication and validation of user access is the major task. Text passwords and graphical image passwords are not secure as there is a chance of shoulder surfing problem. So in order to overcome this problem we are proposing an efficient algorithm for secured services authentication. The algorithm mainly deals with Images and Visual Cryptography. In this paper, at the time of new registration, user provide email id and then image of the applicant's choice. Image given as input is processed in such a way that, particular selected image by applicant is taken as input and is divided into two shares and then encrypted. One share is preserved in the service provider's database and other share is sent to the applicant's email id. The applicant need to provide share during every transaction and that share is over lapped with the already existing share in service provider's database and verification of data for authentication will be done. If username, password and uploaded encrypted image share got matched with existing database details, then the authentication is said to be succeeded.

Keywords: Authentication, Hacking, Visual Cryptography, Image Based Authentication.

I.INTRODUCTION

In protecting privacy of humans from hackers authentication plays a major role. Authentication [1] is the process of verifying the identity of a user so that the user becomes known by the system. Access is denied to users those who fail to authenticate successfully, thereby eliminating the threat of malicious clients posing as legitimate network users. For users who authenticate successfully, we can define policies that enforce usage rules and standards. We can also leverage our existing user groups to enforce policy. Process of determining which resources a user or group can access called authorization which can only occur after successful authentication. We can also configure the appliance to log the activities of authenticated users so that we can

monitor user activity in logs and reports. This allows you to assess how well your policies are working or track down users who are misusing resources or exposing your network to potential threats.

There are authentication techniques like text password based authentication, graphical image authentication, biometric authentication, image based authentication and so on. Mostly now a day's authentication system in use is text related passwords. But, text passwords are insecure for most of the applications that use security by access control mechanisms.

Authenticating through text based passwords has some drawbacks. Some secured text password related authentication processes are costly and may require some hardware. In graphical password system authentication is by clicking on images rather than typing text. Categorized techniques of graphical password system are Recognition Based Techniques and Recall Based Techniques. But there is a problem of shoulder sniffing problem with graphical passwords. Biometric authentication is an expensive process as it requires a hardware. So here to overcome all these drawbacks we are going through a system that use image based authentication using visual cryptography.

Image based authentication is based on a user's successful identification of image password set. User is given a image share at the time of registration and during authentication user have to provide the image share correctly to get authenticated. We are using visual cryptography technique for secure authentication. Visual Cryptography technique involves encryption of image and that encrypted image is divided into some shares and decrypting those shares and overlapping will give us the original image. Image password is easily remembered than string of character password and is more secure. Image based authentication is less vulnerable by attacker.

Visual cryptography scheme(VCS) is proposed by Naor and Shamir [2]. Visual cryptography(VC) is the scheme used for the secrete share of image, in that secret share the original image is divided into number of shares and that share is distributed to some number of participants as each to one. That secret image is recoverable only when participant share their secret.

Visual Cryptography System divides image into random shares and information of shares is not revealed but only size of share can be known. We get the original image by stacking shares. Visual cryptography encodes binary image into n shares of random binary patterns. The image can be visually decoded. This cryptographic encryption technique involves pixel shuffling and inter changing their position to create the ciphered image, this proposed method makes it difficult for decryption of the image without prior knowledge of the algorithm.

II.RELATED WORK

A lot of analysis has been done on secure authentication using visual cryptography and however no one gave secured image authentication. Here in this section we give explanation related to visual cryptography. We discuss about traditional Visual Cryptographic Scheme [3]. In traditional VCS any one of shared image recover the original image which is not secure.

Segment based VC [4], encrypts only symbols and numbers. VCS proposed by Wei-Qi Yan et al[5], can be only useful for printed text or image. If user reveals image share to any other person and trusting that person wont cheat is not true always.

So cheating prevention methods are proposed by Yan et al,[6], Horng et al,[7], Hu et al,[8] but there is no authentication testing. Authentication testing done but this proposed system use signature image which is not so secure and require external hardware which becomes an expensive authentication process. After all the analysis a system is proposed which is a secure authentication scheme.

III.METHODOLOGY

During Internet banking registration time user is asked to select any image of his choice. That image is taken as input. Input image is encrypted and is divided into two shares, One will be sent to bank user's email id provided during registration and another will be sent to regarding bank. The original image stored in respective bank database, and one share sent to bank is also stored in bank database. When user want to login and do any transaction then user must upload secrete share image. Once the correct image share is uploaded while login then user share and bank database share is stacked and the stacked image is decrypted. After decryption if the image matched with the bank database original image then we can avail all the services that banking site provide. In this methodology there are two phases.

A. Registration Phase

During Registration user have to upload an image of user choice. That uploaded image is encrypted and then divided into two shares. One share is sent to users email id and other share is stored in bank server database. Original image is also stored in bank database that was uploaded at the time of user registration. The procedure is shown in figure 1.

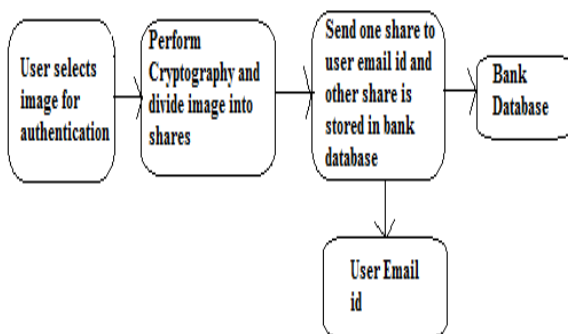


figure 1. User Registration Process

B. Login Phase

In login page user enters his unique id along with his share. Then the database share is overlapped with user share and if got matched with original image after decryption then login is said to be successful. figure 2 shows the procedure.

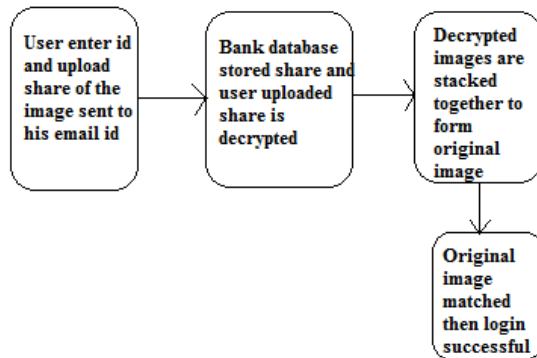


figure 2. User Login Process

For encryption and decryption of image we are using RSA Algorithm[11].

RSA algorithm is complete public key cryptosystem [9, 10]. This paper applies the RSA algorithm for information hiding to secure the user information. RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent. The steps for RSA algorithm are:

- (1) Find two large primes p, q .
- (2) $n = p * q, z = (p - 1) * (q - 1)$.
- (3) Select a number e which is less than n and prime to z , so that e and z have no common factors.
- (4) Select another number d , where $(e*d-1)$ is divisible by z .
- (5) The public key is (n, e) and the private key is (n, d) .
- (6) For a message m , if the cipher text is c , decryption and encryption process as follows:

Encryption: $c = m^e \bmod n$.

Decryption: $m = c^d \bmod n$.

Data is embedded into encrypted image by using Least-Significant-Bit(LSB) method.

Algorithm to hide the data in encrypted image using LSB method:

STEP-1: Consider an encrypted image (cover image).

STEP-2: Consider the message or data that should be hidden into the cover image.

STEP-3: Convert all the pixel values of the encrypted image from grayscale to binary (8-bit).

STEP-4: Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.

Thus, the image encryption is obtained. Decryption done by doing the reverse of encryption.

IV. ALGORITHM

An **algorithm** is a sequence of unambiguous instructions for solving a problem, i.e., for obtaining a required output for any legitimate input in a finite amount of time. Algorithm flowchart shown in Fig 3.

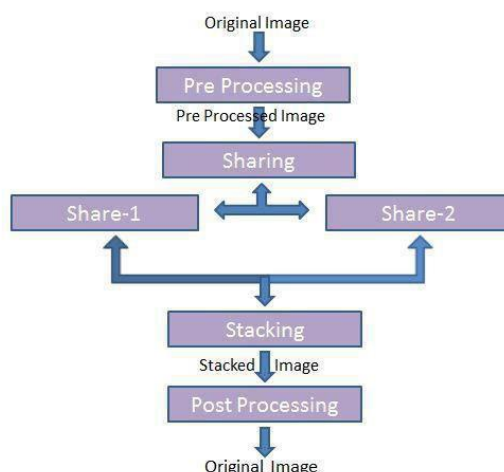


Fig: 3 System Architecture

In this algorithm, the first step is pre-processing. In this step the input image is uploaded during registration process. In the second step, input image is encrypted and the encrypted image is divided into two shares and one share is stored to bank database and other share is sent to user email id. In third step, reconstruct shared images and it will be construct single image. In the fourth step an encrypted single image has to be decrypted to get original image. Fifth step is final step and in this step system authenticate the user is valid or not.

1.Pre-Processing:

In Pre-Processing state image is taken as input shown in below Fig:4. is encrypted by using Visual Cryptography System (VCS).



Fig: 4 Original Image.

Image in the fig: 4 uploaded by applicant during registration will be encrypted using regarding VCS technique. In this encryption image converted to binary format. The encrypted form of fig: 4 is as follows

[illegible]

Fig: 5 Encrypted image.

2. Creation of Shares:

Encrypted image in Fig:5 is divided into two shares as shown in below Fig:6.

1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101
1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101
11001100110011001100110011	11001100110011001100110011
00110011001100110011001100	00110011001100110011001100
1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101
1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101

Fig: 6 Encrypted image shares.

3.Stacking

When user want to transaction, then he/she should be upload a shared secrete image. Later it will pass through the stacking state. In Stacking the bank image share and user share, two images are overlaps and combine both as single image that also encrypted. Combine two images shown in Fig:6 into single image as shown in below Fig:7.

1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101
1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101
11001100110011001100110011	11001100110011001100110011
00110011001100110011001100	00110011001100110011001100
1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101
1010101010101010101010101010	1010101010101010101010101010
0101010101010101010101010101	0101010101010101010101010101

Fig:7 Stacked Image

4.Post-Processing:

The overlapped shares results in required image with randomly distributed redundant information. After completed Stacking state, post processing state taken input as encrypted overlap image. In this state decrypted the overlapped image by using VCS technique.

[illegible]

Fig: 8 Decrypted image.

Whenever two shares are stacked the resulting image is checked for authentication. Whenever two shares of different images are overlapped then the overlapped image validate for authentication. In authentication if it will return true then transaction should done otherwise it will abort transaction. On successful authentication we get original image in Fig 9.



Fig: 9 Authenticated Image

The creation of image share algorithm and authentication process algorithm shown in Alg1 and Alg2. Alg1 shows the creation of shares. Alg2 shows the authentication process.

Alg1: Creating Image Shares

begin

content=read image()

fs=content.size()

ff content odd

content+1

firstshare=contentdata/2

secondshare=content- firstshare

sf firstshare & secondshare

setresimg=1

else

setresimg=0

End

Alg2: Authentication Testing

Begin

secondshare=usershare

firstshare=bankshare

add firstshare,secondshare

```
if originalimg==img
    authenticated
else
    not valid
end
```

V. FUTURE ENHANCEMENT

In this paper we developed enhancement is offline transaction. Mostly transactions are done through online only.

Hence, the system has been implemented as per the requirement of the client. However it can be extended to few more and we can provide feature for the client. During login the client if he/she wants to change image which was submitted in register form he/she can select new image, the new image was updated in the database.

VI. CONCLUSION

Image segmentation is secured because of divide and sharing image shares between user and database. This system is user-friendly and has simple interface. Provide strong security against both attacks and hackers. Protects system vulnerable to attacks.

VII. REFERENCES

- [1] "Authentication and Authorization" from SANS Institute InfoSec reading room.
- [2] M. Naor and A. Shamir, "Visual Cryptography". *Advances in Cryptography-EUROCRYPT'94*, Lecture Notes in Computer Science 950, 1995, pp. 1-12
- [3] "Visual Cryptography Schemes for Secret Image" N. Anusha, P. SubbaRao, *International Journal of Engineering Research & Technology(IJERT)* Vol. 1 Issue 5, July – 2012.
- [4] B. Borchert, "Segment Based Visual Cryptography". WSI Press, Germany, 2007.
- [5] W-Q Yan, D. Jin and M. S. Kanakanahalli, "Visual Cryptography for Print and Scan Applications". *IEEE Transactions*, ISCAS-2004, pp.572-575.
- [6] H. Yan, Z. Gan and K. Chen, "A Cheater Detectable Visual Cryptography Scheme," *Journal of Shanghai University*, vol. 38, no.1, 2004



- [7] G. B. Horng, T. G. Chen and D. S. Tsai, "Cheating in Visual Cryptography," *Designs, Codes, Cryptography*, vol.38, no.2, 2006, pp.219- 236.
- [8] C. M. Hu and W. G. Tzeng, "Cheating Prevention in Visual Cryptography," *IEEE Transaction on Image Processing*, vol. 16, no. 1, Jan- 2007, pp. 36-45.
- [9] Cryptographic and N/W security: Principles and Practices by Stalling. Prentice Hall. 2nd Edition.
- [10] Sos Agaian and Yicong Zhou. 2011. "Image Encryption using the image Steganography concept and PLIP model". IEEE International conference on System Science and Engineering. pp. 699-703.
- [11] Gunasekaran G. and Bimal Kumar Ray. "ENCRYPTING AND DECRYPTING IMAGE USING COMPUTER VISUALIZATION TECHNIQUES" , Vol.9, No.05, May 2014, pp.646-650.