SECURITY IN E-BANKING USING VISUAL CRYPTOGRAPHY TECHNIQUE

[1]ANKITA AROTE, [2]ASISH PANDEY, [3]DIPIKA GUNJAL, [4]PRADNYA DILPAK

Computer Amrutvahini College of Engineering, Sangamner
Email: ankita.arote22@gmail.com, asishkrpandey2910@gmail.com

Abstract— the dramatic increase in computer usage has given rise to many security concerns. Thus security has become most important aspect in today's online transactions. Many verification and validation algorithm are used today to avoid such a security threats. One of them is Visual cryptography. One of the important threats is phishing attack. In our project we have shown how visual cryptography is used to avoid phishing attack for any user doing online shopping. Visual cryptography is an image based security providing algorithm. In Visual Cryptography the original image is preserved or secured by decomposing it into n shares.

Keywords— Phishing, Visual Cryptography Scheme, Shares, RSA, Encryption, Decryption.

I. INTRODUCTION

Whole world now does online shopping or any sort of online transaction. As today online transactions are very common in same way various online attacks are also very common. In general, authentication techniques can be classified as knowledge based, token based and biometrics. Knowledge based means in this user need to remember any sort of text or graphical password. Knowledge based techniques are further classified as recall and recognition based. In recall based techniques user has to recall the secret password created before. While in recognition based user requires to identify or recognize the secret password. To have more security recognition based techniques are used.

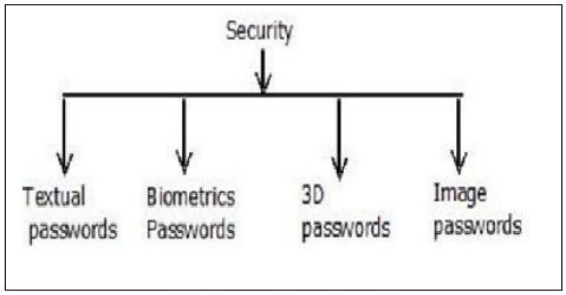


Fig. 1. Type of securities.

Phishing attack is one of such important security threat today everyone is facing. Phishing does not mean hacking but it is stealing of sensitive information of a person e.g. password or credit card credentials. While fishing in sea or lake we try to capture fish, in the same way in phishing phisher try to capture persons credentials. It can be define as "a game that scammers use to collect personal information from unsuspecting users". Visual cryptography is a cryptographic technique in which one encrypted message can be decrypted only by human visual system. Visual cryptographic technique can be utilized by image blurring then thresholding and then encrypting it. We have used recognition based technique. In this project we have comprehensively analyzed and discussed the visual cryptography. In this paper we have shown our project design and how image can be used as password for online transaction. Steps taken to process the image and generate shares of image are discussed in detail in below sections.

II. SURVEY

For this approach we have studied different books and IEEE papers. Concept of visual cryptography is referred from. This concept is again discussed in section III. The reference surety algorithm that's RSA is taken from. And explained shortly in section V. Image processing part is studied from [1]. Necessary details required for project are then discovered in section VI.

III. VISUAL CRYPTOGRAPHY

Visual Cryptography is secure technique for detecting fake websites and phishing attacks caused by it. It is method of sending and receiving the messages that can be decrypted only by sender and receiver. Naor and Shamir introduced this technique as simple and secure way of sharing secret image as password. There are two parts in this technique viz. Encryption decryption and image share generation. The encryption and decryption of message is done by simple mathematical algorithm. The second important part in this scheme is share generation of the image. VCS is a cryptographic technique that encrypts of visual information such that decryption can be performed using the human only. We can use this technique by applying
One of the following structure schemes:

A. (2,2) Threshold VCS schemeIt the simplest scheme that generates two shares of one image. User need to have these both shares for while obtaining original image.

B. (n,n) Threshold VCS scheme Here we generate n shares of the image. When all this n shares are combined then only secret image will get revealed. One missing can let us obtain secret image.

C. (K,N)Threshold VCS scheme Here we generate n shares of the image. But the secret image is revealed only when we get group of at least k shares.

IV. ARCHITECTURE

In this section we will study the block diagram of the system. Here we have designed whole transaction into two phases named:

A. Registration Phase:

For any online transaction or shopping we first need to have account in any bank. In this phase we provide some identity information to bank. Now we are using RSA algorithm we also set public and private key for our account. The fig1 below shows stepwise execution of this phase. Fig.1. Below shows how user registers in bank. In this we have seen that public key is to user and private is kept with bank.

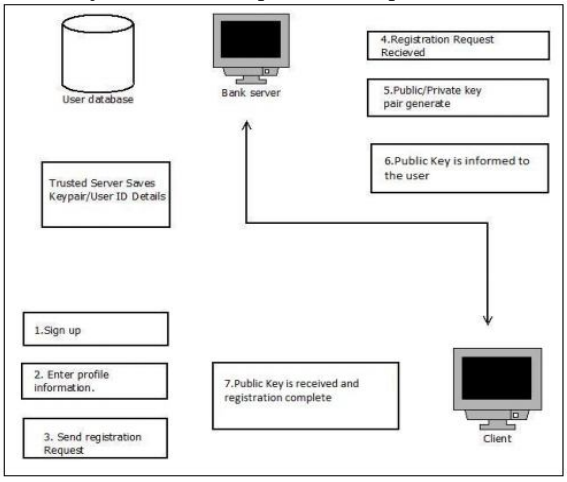


Fig. 5. Registration Phase.

B. Transaction Phase:

This phase is actual transaction activity between user, merchant server and trusted server. Here image processing is done. The steps that are executed are as shown in fig 3. Above.

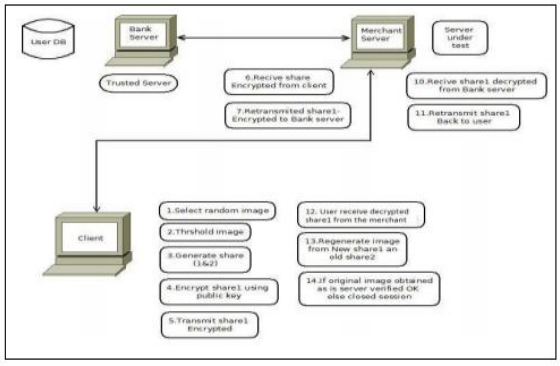


Fig. 6. Transaction Phase

We have made slight modification in this phase of VC. Here user can change his image password every time he need. User can select any random image he has as his password. This makes transaction more easy as user don't need to carry the image always where ever he go as he can change it always. Trusted server have its own database were it stores users as always as merchants information. Any faulty merchant website can be identified by bank. And accordingly phishing can be prevented and stopped. Unless doesn't obtain the original image after decryption the transaction won't be completed.

V. RSA

RSA stands for Rivest, Shamir and Adleman. RSA is most widely used for Public-key Cryptography algorithm. It primarily consists of two blocks of texts plaintext and ciphertext. In our project we have used RSA algorithm for two main activities i.e. Encryption and decryption of image. Fig. 4 Shows how it is done. This provides authentication required for transaction.

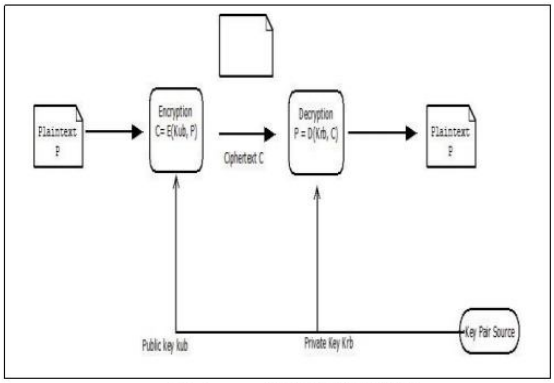


Fig. 7. Authentication in RSA

RSA is a block in which plaintext and cipher texts are nothing but integers ranging from 0 to n-1 where n are some number. .RSA involves three steps sequentially key generation, encryption and decryption. In this technique one uses public key to encrypt and the other uses private key to decrypt the data. Algorithm steps are as follows:

A. Key Generation:

1) Select any two distinct prime numbers p and q, $p \neq q$.
2) Compute n= p*q, where n is modulus.
3) Then compute φ (n)= (p-1)(q-1), where φ is Euler's totient function.
4) Choose integer e such that $1 < e < \varphi(n)$ and $\gcd(\varphi(n),e) = 1$. Where e is released as Public key.
5) Compute $d = e \pmod{\varphi(n)}$, where d is released as Private Key
6) Get public key as KU = {e, n}.
7) Get private key as Kr = {d, n}.

B. Encryption:

To obtain ciphertext, plaintext blocks P<n is used as:
C= Pe mod n.

C. Decryption:
To obtain plaintext, ciphertext block C is used as:
P= C dmod n.

RSA is more secure because factoring of big number n is difficult. Hence it is also difficult to obtain φ (n). Without obtaining φ (n) it is difficult to steal the data or credential of user. One advantage of RSA is that it can be used for both encryption and digital signature. There are different types of attacks those try to break RSA security algorithm. Brute force attack is one of them. But it is time taking. Till phisher try to break our security user can change the image multiple times and efforts of phisher will be wasted. Thus changing the image multiple times whenever required is the best part of our architecture.

VI. IMAGE THRESHOLDING

In this approach of ours we have image as password. We are dividing image into n number of shares to use them as secret password. Image is collection of pixel. Image can be 2D array. And pixel again is smallest visual element as shown in fig 5. Pixels are stored in form of integers. Formats can 8b, 24, and 32bits. .

Fig. 8. Pixel

The most popular color format is 24bits RGB format in which 8 bits of red, green and blue of each colors are present. 8bit images are nothing but grayscale images. Grayscale images are mainly used for image processing. They are different then black n white images. In our approach we first convert color image into grayscale image which is then converted into black and white. The n shares are generated from this black and white image. And used as password.

A. Conversion of color image into grayscale image:
The very first step of image processing is conversion of RGB 24bit image into grayscale 8bit image. The following steps show it is done:

a) Traverse the complete color image and its pixel value. This pixel value will be 24bit.
b) Now split red, green and blue colors by right shifting the pixel value by 8 bit and then perform logical AND operation with hexadecimal 15 as below
B = pix & 0ff
G= (pix>>8) & 0ff
R= (pix>>16) & 0ff
c) Now calculate grayscale component for each red, green and blue pixel value. This is done by taking average of them
Gs=(r+g+b)/3
d) Recompose 24bit value from 8 bit grayscale and save it to new location.

B. Conversion of grayscale into black and white:
This process is also known as image thresholding it is simplest image fragmentation technique. Here we convert necessary features of image into white pixel and rest part into black pixel. As we known black and white image is binary image. Algorithmic steps for this will be as follows:
a) Traverse entire grayscale image. And read each pixel value.
b) Calculate the binary into for it as If gs value is < then th
Then pixel =0 (black)
Else pixel =1(white)
c) Save image into new location.

C. Share generation from binary image:

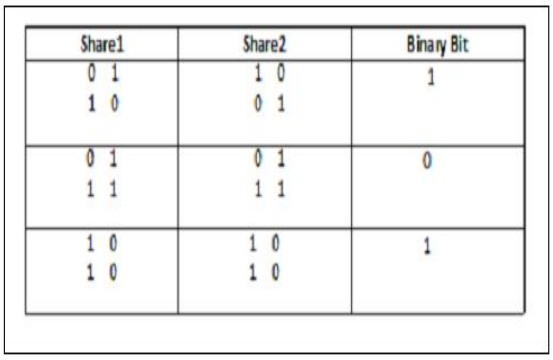
Binary Bit	Random Matrix	Share1	Share2
1	0 1 1 0	0 1 1 0	1 0 0 1
0	0 1 1 1	0 1 1 1	0 1 1 1
1	1 0 1 0	1 0 1 0	1 0 1 0

Fig. 9. (2,2)Share generation scheme

In this approach we divide image into n shares. Here we have shown 2 shares generation. For input binary image which is in 1 and 0 format. Here for each pixel we generate one 2*2 matrix. Generation of share is as shown above. Here we one random 2*2 matrix is generated which is then considered as share1.
In case when binary pixel is black the share 2 is generated by interchanging the columns of matrix as shown in above fig 6. In case when binary pixel is white the share 2 is same as that of share1 Next by comparing two shares we generate binary image. If share are similar then pixel white is generated. If different then pixel black is regenerated.

Fig. 11. Pictorial representation of share generation

When the transaction comes to end the user have check the originality of merchant. At this time he needs to overlay the shares to obtain original image. This can be done as shown below in fig 8.



Share1	Share2	Binary Bit
0 1 1 0	1 0 0 1	1
0 1 1 1	0 1 1 1	0
1 0 1 0	1 0 1 0	1

Fig. 12. Obtaining original image

Thus in this way we have seen all image processing techniques.

CONCLUSION

The proposed method preserves confidential data. As seen above is very easy to use and secure way to keep credentials. User can make it potable.

All that user need is internet connection and image generation app in his gadget. Its overcomes many drawbacks of recently used textual passwords methods. Hence visual cryptography is best to avoid phishing attack.

REFERENCES

[1] Sagar Kumar Nerella Kamalendra Varma Gadi RajaSekhar Chaganti, "Securing Images Using Colour Visual Cryptography and Wavelets," International Journal ofAdvanced and Research in Computer Science and Software Engineering, volume 2, issue 3 March 2012.

[2] Divya James,Mintu Philip,"An Novel Antiphishing framework based on Visual Cryptogyaphy" International Journal of Distributed and Parallel Systems (IJDPS), Vol.3, No.1, January 2012

[3] William Stallings, CRYPTOGRAPHY AND NETWORK SECURITY, 5th ed.,Pearson, 2011, pp 301-320.

[4] Jenila Vincent M., E.Angeline Helena, "Securing Multiple Color Secrets Using Visual," Procedia Engineering, 2012, pp. 806-812.

[5] Moni Naor Adi Shamir,"Visual Cryptography," unpublished.

★★★