SECURE E-BANKING APPLICATION BASED ON VISUAL CRYPTOGRAPHY

Yogesh Kore[1], A. G. Patil[2], Aishwarya Hasbe[3] ,Anuja Chougule[4], Ajinkya Sakale[5]

[1]B.Tech IV, E&TC, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India.
[2]Assistant Professor,E&TC, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India.
[3] B.Tech IV, E&TC, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India.
[4] B.Tech IV, E&TC, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India.
[5] B.Tech IV, E&TC, Padmabhooshan Vasantraodada Patil Institute of Technology, Budhgaon, Maharashtra, India.

---***---

Abstract - *There are numerous security issues as a result of the sharp rise in computer use. As a result, security has taken the top spot in today's internet operations. To prevent such security risks, numerous verification and certification algorithms are used today. The visual encryption is one of them. The phishing attack is one of the significant dangers. In our initiative, we've demonstrated how visual encryption can protect online shoppers from phishing attacks. A security-providing program that uses images is called visual encryption. The initial picture is secured or kept in visual cryptography by being divided into n shares.*

Key Words: *Phishing, Visual Cryptography Scheme, Shares, RSA, Encryption, Decryption.*

1. INTRODUCTION

Nowadays, everyone in the globe does business online. Online crimes of all kinds are as prevalent as online interactions are in today's world. The three main categories of verification methods are knowledge-based, token-based, and fingerprint. Knowledge-based security requires the user to recall any text-based or graphic passcode. Techniques that rely on knowledge can also be categorized as memory or identification based. In recall-based methods, the user must remember the previously established private password. The user must be able to determine or recognize the private password in recognition-based systems. The use of recognition-based methods is increasing protection.

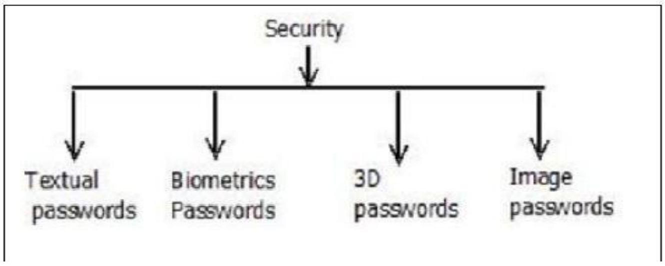


Fig -1: Type of Securities

One significant security risk that everyone is currently exposed to is phishing attacks. Phishing is the theft of a person's private information, such as a password or credit card information, and does not correspond to cybercrime. In the same way that we attempt to catch fish when we go lake or sea fishing, phishers try to grab people's credentials when they send out phishing emails. It is a "game that scammers use to steal personal information from unwary users," according to one definition. One encrypted communication can only be decoded using the human vision system when using visual cryptography. It is possible to use a visual cryptographic method by thresholding, blurring, and then encrypting a picture. We used a method that is based on recognition.

We have thoroughly examined and discussed visual cryptography in this project. This paper demonstrates our project design and the use of images as passwords for online transactions. The procedures used to create shares of the picture and process the image are covered in depth in the parts below.

2. LITERATURE SURVEY

For this approach we have studied different books and IEEE papers.

2.1 Black and White VC Scheme

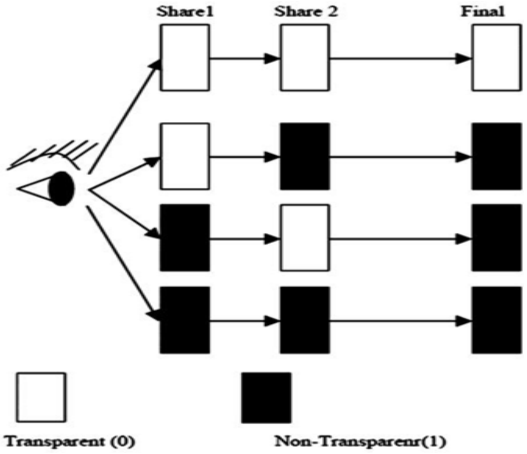


Fig -2: Human Visual System as OR Function

The encoding method suggested by Naor and Shamir [1] divides a binary picture into two shares, Share1 and Share2. Fig.2 top two rows are selected to produce Share1 and Share2 if pixel is white. Similar to this, Share1 and Share2 are generated if a pixel in the bottom two rows of Fig.2 is dark. Since each share pixel p is split into two white and two black pixels, neither share by itself can reveal whether a pixel p is white or black. Only when both files are superimposed will the secret picture be visible. Stacking shares illustrates an OR procedure. OR is a lossy restoration procedure. We can get a lossless restore of the original picture if the XOR operation is used in place of the OR operation. However, XOR operation requires calculation. The OR procedure can only be simulated by the actual stacking process.

This method has the following shortcomings:

- It only works with black and white pictures.
- Shares are four times larger than the original picture, requiring more storage space.
- As each cycle requires the encoding of a single image, it takes time.

2.2 Color Visual Cryptography Schemes

Chang and Tsai anticipated color visual encryption strategy for sharing a secret color picture and also for generating the meaningful share to send a secret color image. For a secret color image, two important color images are chosen as cover images that are the same size as the secret color image. The secret color picture is then concealed into two camouflage images using a preset Color Index Table. One disadvantage of this strategy is that additional space is needed to build the Color Index Table.

Similar to the Verheul, Van Tilborg, Yang, and Laih [3] schemes, the number of sub-pixels in this scheme is proportional to the number of colors in the hidden picture. The size of shares will increase as the secret picture contains more colors. Chin-Chen Chang et al [4] created a private color picture sharing system based on modified visual encryption to overcome this restriction. This plan offers a more effective method to conceal a gray picture across various shares. In this system, the size of the shares is set; it does not change depending on how many colors are visible in the hidden picture. There is no need for a preset Color Index Table with Scheme.

3. VISUAL CRYPTOGRAPHY

Visual cryptography is a safe method for spotting fake websites and the phishing attacks that are brought on by it. Only the sender and recipient can decode the messages using the method of transmitting as well as receiving messages. This method was developed by Naor and Shamir as a quick and safe means to share a password-protected secret image. This method consists of two steps: picture share creation and encryption decryption. Messages are encrypted and decrypted using a straightforward mathematical formula. The creation of the picture shares is the second crucial component of this scheme.

VCS is a cryptographic method that encodes visual data so that only a human being is able to perform the decryption. Applying one of the following methods, we can use this technique:

A. (2,2) Threshold VCS scheme it 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.

4. RESEARCH METHODOLOGY

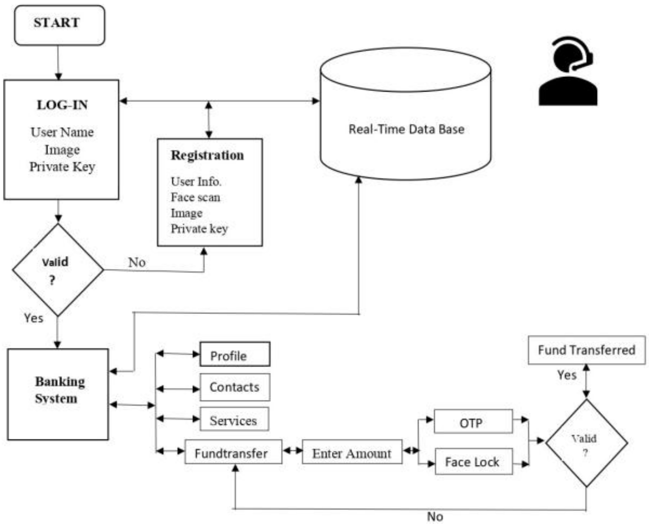


Fig -3: Architecture of E-banking System

In this section we will study the block diagram of the system. We have divided the entire transaction into two phases, which we have labeled:

4.1 Registration Phase:

For online transactions and purchases, you must first open a bank account. At this stage, you provide your bank with your identity information. We are using the RSA algorithm and also set the public and private keys for your account.

Also we need to scan thumb and face which will be used during login as extra authentication option. Above Fig.3 shows the step-by-step execution of this phase. It shows how a user registers with a bank. In it, the public key belongs to the user and the private key is kept in the bank.

4.2 Transaction Phase:

Actual interaction between the customer, the merchant server, and the trusted server occurs during this stage. Here the image processing is done. The actions are carried out in the order depicted in Fig. 3. above. In this VC version, we have implemented a few minor changes. After entering amount user will receive OTP, and if the opt is correct then thumb scanning will be done. All this steps are authenticated and if they are valid then transaction will be done. Trusted servers have their own databases where they keep records of both vendor and customer information. Bank is able to determine any problematic vendor website. Phishing can be avoided and halted as a result.

5. RSA

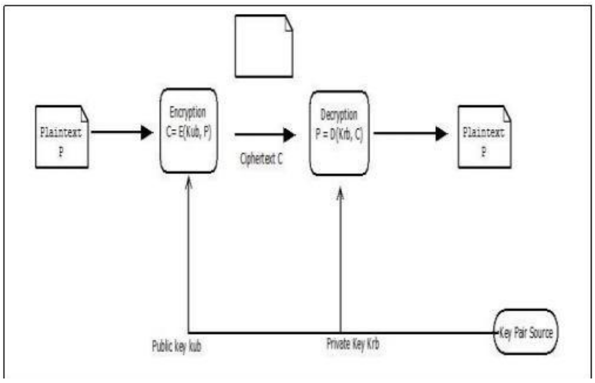


Fig -4: Authentication in RSA

Rivest, Shamir, and Adleman is referred to as RSA. The most popular public-key cryptography method is RSA. It mainly consists of two blocks of text, the plaintext and the cipher text. In our project, we used the RSA algorithm for the two main activities: image encryption and decryption. Figure 4 illustrates the process. This offers the necessary verification for the transaction.

Plaintext and encryption texts in the RSA block are nothing more than numbers in the range of 0 to n-1, where n is a certain number. Key generation, encryption, and decryption are the three consecutive stages in RSA. In this method, one party encrypts data using a public key, and the other party decrypts it using a private key. These are the stages of the algorithm:

5.1 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(mod φ(n)), where d is released as Private Key
6) Get public key as KU = {e, n}.
7) Get private key as Kr = {d, n}.

5.2 Encryption:

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

5.3 Decryption:

To obtain plaintext, cipher text block C is used as:
P= C dmod n.

Because it is challenging to calculate large numbers, RSA is safer. Due to this, obtaining φ(n) is also challenging. It is challenging to take a user's data or credentials without getting φ (n). The fact that RSA can be used for both cryptography and digital signatures is a benefit. There are many attacks that aim to break the RSA security code. One of them is the Brute force attack. But it takes effort. User can alter the picture numerous times until phisher attempts at breaking our security are useless. The greatest feature of our design is that it can change the image numerous times as needed.

6. IMAGE THRESHOLDING

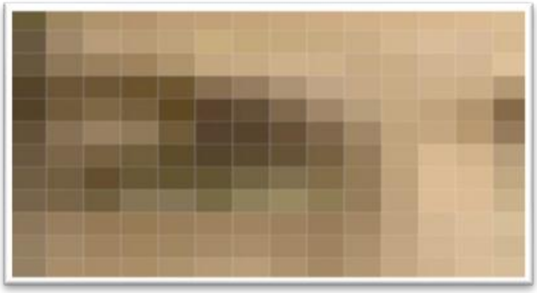


Fig -5: Pixels

Our approach uses images as passwords. Split the image into n shares to use as a secret password. An image is a collection of pixels. Images can be 2D arrays. Again, pixels are the smallest visual elements, as shown in Fig.5. Pixels are stored in integer format. Formats are 8b, 24, and 32 bits.

The most common color code is the 24 bit RGB format, which contains 8 bits of each red, green, and blue color. An 8-bit image is just a monochrome image. The majority of picture analysis uses gray scale images. They are distinct from black and white photos. In our method, color images are first transformed to monochrome, which is then changed to black and white. This black and white picture produces the n shares as a passcode, also.

6.1 Conversion of color image into gray scaleimage:

Converting an RGB 24-bit picture to a gray scale 8-bit image is the first stage in the image processing procedure. The methods below demonstrate how to done:

a) Go through the entire color picture and each pixel's value. This pixel number has a 24 bit width.

b) Next, divide the red, green, and blue colors by right shifting the pixel value by 8 bits.

Finally, use hexadecimal 15 to execute the logical AND operation as shown below.

B = pix & 0ff

G= (pix>>8) & 0ff

R= (pix>>16) & 0ff

c) Next, compute the gray scale component of each red, green, and blue pixel value. This is done by averaging Gs=(r+g+b)/3
d) Reconstruct 24-bit values from 8-bit gray scale and save to new location.

6.2 Conversion of gray scale into black and white:

This method of picture segmentation is also referred to as image thresholding. Here, we change the essential aspects of the picture to white pixels and the remaining portions to black pixels. As is common knowledge, binary images come in black and white. The following algorithmic methods will be used for this:

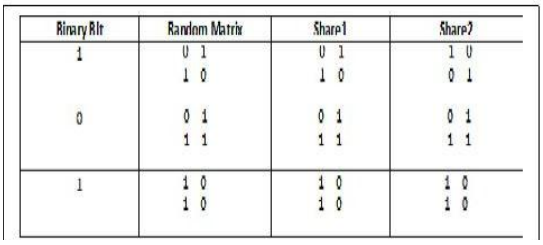
1. Determine the threshold value, T.

2. Make a duplicate of the original Image Array (let's call it “binary") with the same number of rows and columns but with all components set to 0. (zero).

3. If the gray level pixel at (i, j) is higher than or equal to the threshold value, T, then give 1 to binary(i, j); otherwise, assign 0 to binary.(i, j).

For each gray scale point, repeat the process.

6.3 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 -6: (2,2) Share generation scheme

This method involves dividing the picture into n parts. We have generated 2 shares in this example. For the binary input picture, which is formatted as 1 and 0? Here, one 2*2 grid is generated for each pixel. Shares are generated as indicated above. Here, a single random 2x2 matrix is produced and is subsequently referred to as share1.

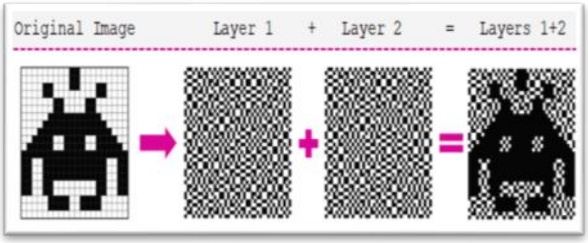
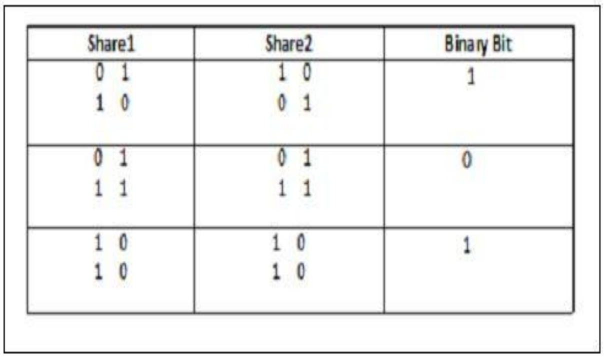


Fig -7: Pictorial representation of Share generation

If the binary pixel is black, the share 2 is created by swapping the columns of the matrix, as shown in fig. 6 above. When a binary pixel is white, share 2 is equal to share 1. Next, we create a binary picture by matching two shares. If the shares are identical, white pixels are produced. If different, black pixels are produced again. The user must verify the authenticity of the vendor when the purchase is complete. To acquire the original picture at this moment, he must overlay the shares. This is possible as illustrated 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 -8: Obtaining original Image

Thus, we have seen each image processing method in this manner.

3. CONCLUSIONS

This system is created using Java technology as a web application.

This method employs Color Image Visual Cryptography to secure passwords, and it is currently technologically hard to defeat this security. The Core Banking Application will benefit greatly from this system, and bank clients will no longer experience password theft issues. Once this system is installed on a web server, every device connected to the network can view it using a browser without needing to install any software.

REFERENCES

[1] Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology–Eurocrypt, pp1-12, 1995

[2] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996)," Constructions and bounds for visual cryptography", in 23rd International Colloquium on Automata, Languages and Programming'' (ICALP '96).

[3] E.Verheuland H. V. Tilburg, "Constructions and Properties of K Out Of N Visual Secret Sharing Schemes." Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.

[4] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998. S. J. Shyu, S.

[5] Y. Huanga, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol.40, Issue 12, pp.3633-3651,2007.

[6] Tao Li, Baoxiang Du, and Xiaowen Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz", 2019 IEEE.

[7] Chandrasekhara & Jagadisha, "Secure banking application using visual Cryptography against fake website authenticity", IJACECT, Vol.02, Issue 02, 2022.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.