Approach for Secure Transaction in Banking Sector Based on Visual Cryptography

Ms. Shital B. Patel [1], Dr. Vinod L Desai[2]
[1]*Research Scholar,RK University,Kastubadham, Rajkot*
[2]*Assistant Professor,Department of Computer Science,Gujarat Vidyapith, Ahmedabad*
(E-mail: patelshital03@gmail.com)(E-mail: vinoddesai123@gmail.com*)*

***Abstract*—**There are lots of problems occurs in all the banking area when they are use computers and internet. Now a day's people use online banking transaction so it must be require security and also banks give surety to provide security for all transaction had done in bank by customer. To obtain this aim of authenticity of user is needed. Only authenticate users can participates in the transaction. In terms of this goal, the banks have uses authentication systems based on biometrics, but because of inevitable basis of malicious activities of the banking system is not safe anymore. Smart hackers can retrieve biometric details Customers from the database of the bank and can use them later for counterfeits Transactions. To avoid all these catastrophic things cryptographic technique is used. Visual cryptography is one efficient encryption scheme in which information is hidden on the Internet images and decrypted only by the human visual system. However, the benefits of e-commerce are considerable. There are some security threats such as debit, credit card fraud, phishing, and so on. In this document, we introduce an electronic payment system. Offers unparalleled security through visual and quantum cryptography.

In this paper visual cryptography technique hides customer details and generate shares while Quantum Cryptography secures the transmission of banking sector.

Keywords*—Visual cryptography, shares, Authentication, Image stacking, XOR.*

I. INTRODUCTION

The banking sector generally uses biometric authentication. Authentication system based on biometrics.

This is done by retrieving raw biometric data such as a face image, fingerprints, etc. From the creative, extracting a feature set from the raw data, and comparing the feature set with the detailed plan stored in the database to authenticate the subject or verify the specified identity. The security of an institution / organization depends on the middleware of the underlying design technology and the design of the database. Any spatial or temporal transaction has an impact on the database. Therefore, hackers are still trying to hack the database. Although the banking system provides basic services to the Web, it is the authentication of the user. Many techniques are used for this purpose, namely password authentication, smart card authentication and the biometric authentication system. All of these techniques are required to manage the database that is vulnerable to hacking. The database contains private information that may cause privacy.1

In this method, the entry is a stored signature image as a whole. However, the goal is to divide this image into a number of divisions containing only a few characters inherited from the original image. The resulting image becomes the subset of the main image. This split technique accepts input types, such as each text image, a drawing image, and a snapshot of a person. If a user may need to open a bank account, he must follow the instructions to enter any information that he may request authentication after signing the user. This is where the visual cryptography function begins [3]. An image is created to be split to separate user and bank divisions. Internally, the original image and the bank partition would be stored in a bank database for the purpose of stacking them to obtain a stacked image overlapping with the partitioning of the user.

This project therefore uses this efficient technique to achieve greater similarity and a positive result. It helps to detect fraud and malicious activity on the web. Finally, there is the optimistic result for better safety back.

In this paper, proposed method uses visual comprehension by textual bases, access to at least information and communication between clients and members of the commission. If this information is protected by the customer and by the user, it is also provided by the customer information. The proposed content is particularly interesting for e-commerce, but it is widely extended for online banking.

The rest of the paper is organized as follows: Section II gives brief description of visual cryptography. Section III contains current system of banking system. Section IV presents proposed method. Section V present Experiment result of proposed method. Section VI concludes the paper.

II. RELATED WORK

Visual cryptography [10] is a secret-sharing scheme in which the secret image is used as an input such as printed, handwritten and the input image encoded in a set of other images, which are called shares so when shares are printed the slides and the original superimposed secret are revealed. The simplest form of the visual Cryptography or visual secret sharing scheme takes the input binary image and manages each pixel independent. To encode a pixel of the secret image, we divide the secret pixel into n versions so that all n versions are printed on transparencies and the original secret pixel is superimposed. This process must be applied to the entire secret image. As a result, parts of the original secret are ready to visualize and superimpose the secret printing of the parts on transparencies. The proposed authentication method uses XOR-based visual cryptography and image processing techniques to authenticate and secure the information stored in the bank database.

One of the cryptographic methods to share secrets images by Naor and Shamir proposed in Visual cryptography. The visual cryptography for a set P of n participants is a method of encoding a secret image (SI) into n ghost images Called actions in which each participant in P receives an action. Some qualified subsets of participants can visually recover the IS, but other groups of prohibited participants have none Information about SI. A "visual recreation" of the qualified ensemble X means they can see the SI by xeroxing the actions Received participants of X on slides, and then they pile up. Thus, participants will participate in a qualified X-Set to be able to see IS without knowledge of cryptography and without cryptographic calculation [1-3].

The VCS describes how an image is located encrypted and decrypted. There are different types of visual elements Cryptographic patterns. For example, there is the k out-of-n system, where n parts are produced encrypt an image and k shares must be stacked for decryption the photo If the number of stacked parts is less than k, the original image is not revealed. Other systems are 2-on-n and on-n-VCS. In the scheme 2-on-n, n parts is generated to encrypt an image and any two actions must be stacked to decipher the image. In the n-off-n Schema, n shares are generated to encrypt an image and n shares must be stacked to decode the image. If the number of stacked parts are smaller than n, the original image is not discovered. The number of shares or participants is increased automatically increase the security of the encrypted Message.

A. Basic Model of Visual Cryptography

In visual cryptography scheme, the secret image is divided into two (n) shared images, so that secret can only be revealed if both parties are stacked together. The Boolean matrices to be sent can be designed in Fig 1.

We can share the white pixel in two parts S1 and S2, as shown in FIG. 1. The S1 share is represented by two combinations of black and white blocks as row 1 and row 2 of 1. The black block stands for 1 and the white one the block represents 0. Therefore, S1 in line 1 is represented by Bit sequence 10 and in line 2 by 01. In the same way, S2 in Rows 1 and 2 are represented by bit strings 10 and 01. Here, the white pixel 0 is divided into two bit sequences according to S1 and S2. When the operation is performed visible between white pixels S1 and S2 at 50% accuracy. However, the reconstructed white pixel is twice as long as the original because of the extent of the pixels. Equally black the pixel is divided into two parts S1 and S2 in rows 3 and 4 from Fig 1.

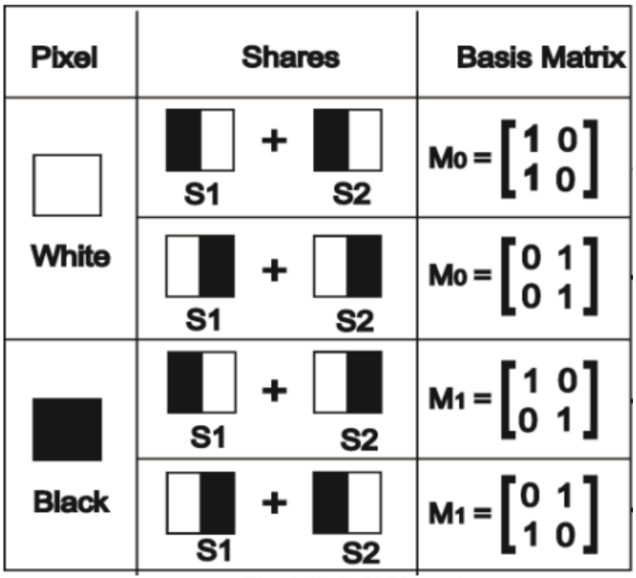
Pixel
Shares
Basis Matrix
White
Black
S1
S2
+
$M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$
$M_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$
$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
$M_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Fig. 1 (2, 2)-VCS$_{OR}$ scheme

This procedure is applied to all the black and white pixels of the window binary image, so two parts are generated. P.S. Revenker et al. [9] had developed the Visually Cryptographic system. All [6] methods are based on the OR operation based on visual cryptography schemes. So generated Inventories have problems with loss of contrast and pixel expansion. Therefore, a lot of space and bandwidth are needed during transmission.

B. Objective

- Confidentiality: The information cannot be understood by everyone who he was involuntary).
- Integrity: The information cannot be changed during storage or during transport between the sender and provided receiver without change get discovered.
- Irrevocability: (creator / sender of the message) the information cannot be rejected later or his intentions in creating or Transmission of information).
- Authentication: sender and receiver can confirm the identity of each and the Origin / destination of the information.

III. EXISTING SYSTEM

In Existing banking system, user open account he get password from bank, but if someone know password or stolen password then anybody can access account of customer. When customer have joint account in a bank so both customer know secure password. If one customer went at bank and access their joint account and easily withdraw money on their account. In joint account any one customer signature is valid for transaction so at that time bank sector need security.

For example, suppose A and B have joint account in bank. Later A get adversarial to B and aspiration to withdraw all the balance from the account. In this situation B is embittered by A.

To solve this problem by using Visual cryptography method. Using this method , when user open his account at that time customer make signature then signature have divided into two part and one part given to customer and other part given to the bank. At the time of withdraw money customer and bank both have submitted secret share, and that share are overlapping at that time they get original signature so bank can identify customer was authorize or not. When Customer have joint account at that time bank created three share and these three share overlap then bank identify he is valid user. Customer have a joint account then all account holder get individual share from bank using visual cryptography scheme. When they want to withdraw money at the not valid if only one user give share, it must be require both customer share and one bank share. All three share are overlap then get original secure password and bank know he is authorize person and last they get money.

IV. PROPOSED METHOD

The suggested method uses Visual Cryptography. Banking systems allow users to interact with services only after logging into the applications they want. If a user wants to open a new account, he / she must first login to the site and open the request form, which the bank already displays as the default format that each user must enter.

The bank uses this form for authentication. It will be recorded as a scanned image. This image itself is an introduction to the system. If the pretreated image and the stacked images are identical after comparison, the user is authorized and allowed access. Otherwise unauthorized and grants no access. This VC method provides complete accuracy in testing the system. This method divides the scanned input image into two parts. One department has to stay with the bank and another is assigned to the user as a department. Since there are two subdivisions, this method is called 2 out of 2 schemes within the pictures.

The preprocessed image and the stacked image become similar, the result is checked and authentication is performed. The flow of the VC technique was shown below Figure 2.

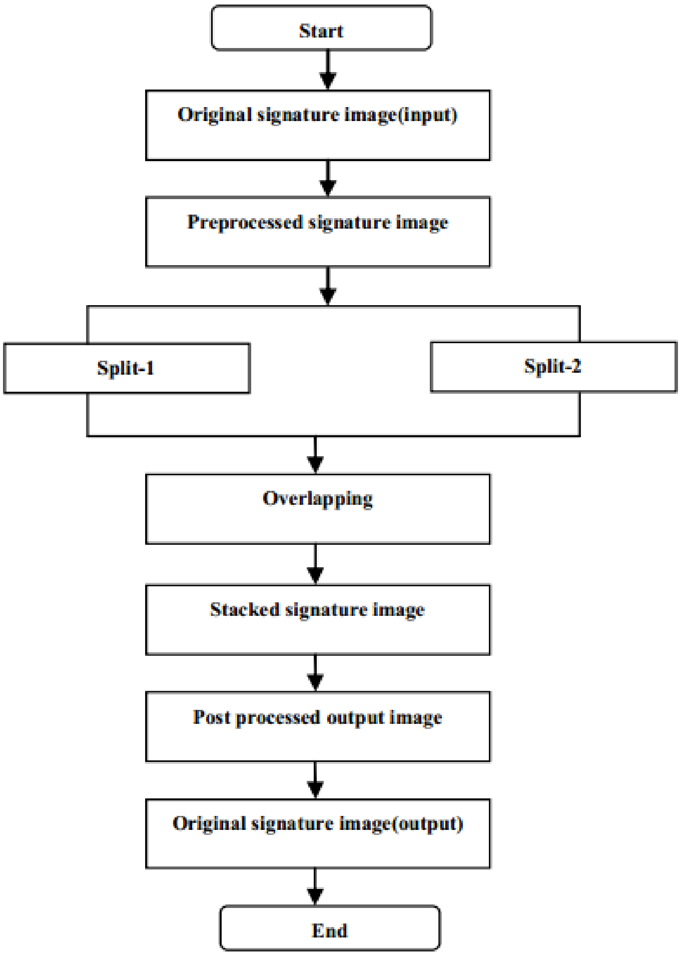
Start
Original signature image(input)
Preprocessed signature image
Split-1
Split-2
Overlapping
Stacked signature image
Post processed output image
Original signature image(output)
End

Fig 2. Data flow diagram of visual cryptography

V. EXPERIMENTAL RESULTS

Figure 3 indicates that the user must first provide authenticated data to the bank administrator. The user provides a digitized signature image to create splits in the next step. This image contains noise in the input data deleted during the preprocessing step. The input image is displayed below fig.3.

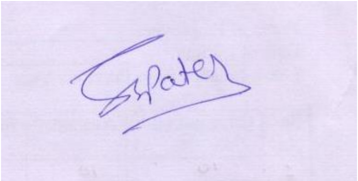

Fig 3. Pre- processed signature image (Input)

In this step, Figure 4 explains that the administrator of the bank creates two departments and the administrator distributes them to the user and to the bank itself. In figure 5 it was explained that the department of the bank is stored in the database of the bank itself. The user must submit a split of the respective user during the transaction transaction, eg. B. withdrawal, deposit or any money transfer. The bank must check whether the user is true and original or not.

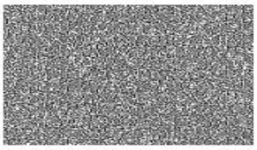

Fig 4.Split-1(User share)

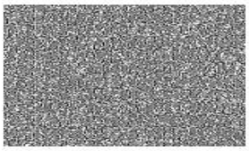

Fig 5.Split-2 (Bank share)

Figure 6 illustrates the last VC step on a post-processed image that is nothing more than a stacked image. The administrator overlaps the two divisions to verify the signature after submitting it to the bank. The stacked image indicates one or more subpixels of the original image. If the image obtained is independent of the subset, it can be explained that it is a false signature and that the user is not a genuine user. If the stacked image corresponds to the input image, it can be said that the user is authorized.

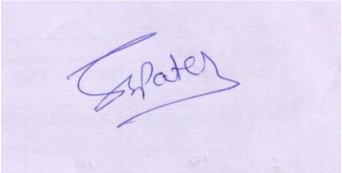

Fig 6. Stacked signature image (Output)

CONCLUSION

In this paper, we proposed a more secure algorithm using visual cryptography. The proposed efficient technique of visual cryptography provides greater security for the stored data on the pictures. The digitized signature image is here an entry in the application for which the bank generates input replicas Image with a VC technique of 2 out of 2. Then the bank shares one division to the user and another is kept in the bank. Database itself. Now, the batching process is performed to compare the pretreated signature with the post processed signature image.

The degree of similarity of the signature determines the acceptance and rejection of the user of the transaction. a service this technique allows secret data authentication and secure transactions to be performed via the online service. This technique can also be applied to photos and color images.

REFERENCES

[1] Jain, A., & Soni, S. Visual Cryptography and Image Processing Based Approach for Secure Transactions in Banking Sector.

[2] Amit R Bramhechar and Dinesh P (2015) "A Survey Paper on Online Payment System using Stegnography and Visual Cryptography with Hidden Markov Model " I International Journal of Modern Trends in Engineering and Research.

[3] S Kumar, B., Brahme, S., Suman, S., Phatak, K., & Pawar, A. M. (2017). "Online Secure Payment System Using Captcha And Visual Cryptography". International Education and Research Journal, 3(1).

[4] Roy, S., & Venkateswaran, P. (2014, March). Online payment system using steganography and visual cryptography. In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on (pp. 1-5). IEEE.

[5] D Gopal, T. V. (2015). Online Payment System Using Steganography and Visual Cryptography. International Journal of Engineering and Management Research (IJEMR), 5(6), 391-402.

[6] Hegde, C., Manu, S., Shenoy, P. D., Venugopal, K. R., & Patnaik, L. M. (2008, December). Secure authentication using image processing and visual cryptography for banking applications. In Advanced Computing and Communications, 2008. ADCOM 2008. 16th International Conference on (pp. 65-72). IEEE.

[7] Roy, S., & Venkateswaran, P. (2014, March). Online payment system using steganography and visual cryptography. In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on (pp. 1-5). IEEE.

[8] Renner, R., & Cirac, J. I. (2009). de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Physical review letters, 102(11), 110504.

[9] R. Navale1 , S. S. Khandagale2, R. A. Malpekar3, Prof. N. K.Chouhan4,"Approach for Secure Online transaction using Visual Cryptography Text Steganography",International Journal of Engineering Research Technology (IJERT) ISSN:2278-0181 Vol. 4 Issue 03, March-2015 894.

[10] Roy, S., & Venkateswaran, P. (2014, March). Online payment system using steganography and visual cryptography. In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on (pp. 1-5). IEEE.

[11] Shital Patel, Dr.V.L.Desai (2016) ―Comparative Study and Analysis of Halftone Visual Cryptography via Error Diffusion‖ in IJARCSSE Vol.6, Issue 1.

Ms. Shital B Patel as a Research scholar in R.K University in Rajkot and Assistant Professor in Department of Computer Science, Ganpat university at kherva. She had passed M.Sc(CAIT) from HNGU at patan.

Dr. Vinod L Desai as a Assistant Professor in Department of Computer Science, Gujarat Vidyapith ,Ahmedabad. He had pass BBA in 2000 at H.N.G.U and passed M.C.A in 2004 at Gujarat Vidyapith and he had awared Ph.D in 2009 at Bhavnagar University.