Survey Paper on Transaction Security in E-Banking Using Visual Cryptography for Joint Account Holders

[1] Mr. Mohd. Akbar, [2] Awadhesh Kumar Rai
[1]Assistant Professor, [2]M.Tech. (Comp. Sc. & Engg.),
[1]Department of Computer Sc. and Engg. ,
[1]Integral University, Lucknow, India

Abstract : In today's banking transaction system security has become the most important aspect because banks are committed to provide secure core banking services to their customers. To achieve this goal authenticity of the users is required only the authorized users can take part in the transaction. For that purpose banks uses biometric based, password based, OTP based authentication systems but due to unavoidable malicious activities like phishing attacks, identity theft, database of the banking system is no longer secure. Smart hackers can fetch biometric details of customers from the bank's database and later can use it for fake transactions. To avoid all this calamitous things Visual cryptographic and steganography techniques along with RSA algorithm is used. Visual Cryptography is a cryptographic technique which allows information to be in encrypted form in such way that decrypted information as a visual image. In this paper we propose a secure XOR operation based visual cryptography and steganography and image processing technique to secure banking transaction.

IndexTerms **- Visual Cryptography, Steganography, E-banking**

I. INTRODUCTION

Online banking has become an emerging trend at present date. As rapid as the online banking increases, the attacks over the online account also increases. security problems such as identity theft and phishing are the major concern for both customers and merchant. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. So many reports were made over these phishing attacks. Such attacks have been noticed to be escalating in the number of attacks along with increasing online customers and sophistication. To provide improved security from leaking of confidential information we need to switch over to an even more reliable protection

scheme to ensure safe networking of transactions. Online bank customers had always been the favourite targets of those who involve in phishing attacks, so that the account details of those customers can fetch them more money in just few seconds.
Apart from that in the case of joint account holders there has been cases when one of the account holder can perform illegitimate actions by doing online transactions. In this paper we propose a new method for E-transactions that provides better security by using cryptographic techniques visual cryptography, and steganography. Visual cryptography hides the authentication details of customer by generating two shares for the joint account holders and bank respectively, the share of the customer is further broken in to two shares and given to each joint account holder. Steganography is used to combine the customer's share along with the one password in order to secure the transmission of customer's share to bank.

Visual Cryptography and Steganography

.
Visual cryptography is a cryptographic technique proposed by Moni Naor and Adi Shamir in 1994.This cryptographic technique encrypts the images in to number of meaningless shares which are Xeroxed in to transparencies and only after combining all the shares generated from the image , the original image is retained.
Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

II. Review of Literature

Table 1: Comparative Study of research work

Sr. No.	Title Work	Research Method	Key Contribution
1.	. ***Mobile Banking App Using Visual Cryptography And Steganography*** by Sejal krishna Gajbhiye, Pooja Gedam, Lavanya Gannamani,Mrunal Deshmukh (2020)	This paper presented two-out-of-two secret sharing visual cryptography method to encrypt colour images. This method breaks input colour image into two parts in a way that only one part is not enough to predict its small portion of original image. Original image can be regained by X-OR operation of both parts	Proposed method does not require complex mathematical calculations. So, the image size of regained image does not increase more and negligible amount of noise is introduced. But, user can see structure of image by overlapping the both parts.
2.	***Enhanced semantic visual secret sharing scheme for the secure image communication*** by John Blesswin A, Christhu Raj, Rajeev Sukumaran & Selva Mary G (2019)	In this paper, introduced Enhanced Semantic Visual Secret Sharing (ESVSS) Scheme that transmits a gray-scale secret image to the receiver using two color cover images. At the receiver end, the secret image is reconstructed by digitally stacking the shares together.	The result analysis shows that the ESVSS achieves security and improves the quality of the reconstructed image. The quality is measured by Peak Signal to Noise Ratio (PSNR) up to +39 dB and Mean Square Error is reduced to 6. The Universal Image Quality Index (UIQI) results are recorded up to 90% for the reconstructed image with minimal computational complexity.
3.	***Cheating Prevention in E-payment System using Visual Cryptography*** Ms. Shital B Patel & Dr. Vinod L Desai (2018)	approach for secure online payment system using Visual Cryptography (VC) and to protect the stealing of data between end users and online merchant website, used Secure Socket Layer (SSL) encryption	This technique shield the customer information to defend the possible forgery purchasing online, When customer opens account in bank, bank will give a private key and this private key divided into two shares. One share will keep bank in its database and other share will give to the customer.
4.	***Online Payment System using Steganography and Visual Cryptography*** Dr.S.Makbul Hussain G. Mahaboob Basha (2017)	Proposed Text Based Steganography Method	Proposed method minimizes customer information sent to the online merchant. Presence of third party CA increased the security further as more number of parties are involved in the process. Usage of steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy.
5.	***Secure E-PAY Using Steganogrphy and Visual Cryptography*** by Sarita swami and Reshma gulwani (2017)	Used an Indian root technique which is a text based steganography and VC	It shares the minimum information to the retailer. Use of CA and merge it applications with steganography and visual cryptography.
6.	***Implementation of secure payment transaction using AES encryption with***	Authentication system Use of OTP generator, QR	It uses visual cryptography and AES encryption to prevent online fraud when an

	extended visual cryptography by Naveen Kumar Kolli (2017)	Code generator, QR code creation, Visual Cryptography on QR code image, XOR based Visual Cryptography, AES encryption on image share	scammer attempts to log in through a payment gatway. In this method it is implemented in two web applications to provide the prototype of actual transactions in the real world.
7.	***Secured Bank Authentication using Image Processing and Visual Cryptography*** by B.Srikanth, G.Padmaja 2016	In this signature of the applicant is scanned as input. It thickens the lighter shades of the image and to increases the intensity of the image by pre-processing. Now pre-processed image is encrypted into shares depending upon the alignment of the black and white pixels and shares are overlapped to decrypt the original image containing the signature.	Pearson's Correlation coefficient is calculated between the original image and the resultant image, if higher correlation coefficient is obtained, them the authentication is succes otherwise not.
8.	***Securing Internet Banking with a Two - Shares Visual Cryptography Secret Image*** by Aparnaa. K. S., Sathyasundaram. M., Santhi. P. (2016)	Uses Visual Cryptography image, Security image for each client. Then that image is split up and used while submission of User Id and password which are made entered in separate web pages to perform the image verification. the first share of the security image stored in Intermediary database the user is asked to answer any one question,after validating the answer with the security text values in Server database, the server discloses the complete Security image.	Delimit the possible Security Images The proposed system creates security images from a text chosen by the user. The text is embedded with some black and white image with lesser contrast and higher brightness such that text is visible to human eye. This technique delimits the limited security image concept of existing system.
9.	***E-Payment System Using Visual Cryptography and Quantum Cryptography*** by Shemin P A ,Prof. Vipin kumar K S (2015)	In this paper E-payment method using quantum and visual cryptography and image steganography is proposed . After opening account, bank will give a private key and one of the shares generated by visual cryptography to customer. Bank will keep other share in its database. Share is generated by applying visual cryptography to snapshot of text containing customer's account number and debit and credit card information. Now customer can perform E-shopping using this share.	This proposed system based on two cryptographic provides unconditional security by preventing man in the middle attack. VC used in this system safeguards the customer's data, where as quantum cryptography and image steganography prevents security threats such as phishing, identity theft.
10.	**Anti-Phishing Structure Based On Visual Cryptography and RSA Algorithm** By Sayali Vaidya, Shreya Zarkar , Prof. Achal N. Bharambe, Arifa Tadvi,Tanashree Chavan	To detect the phishing website used registration Phase and Login Phase using VC and RSA algorithm	Anti-phishing Structure Based on Visual Cryptography and RSA Algorithm, phishing websites can be identified.

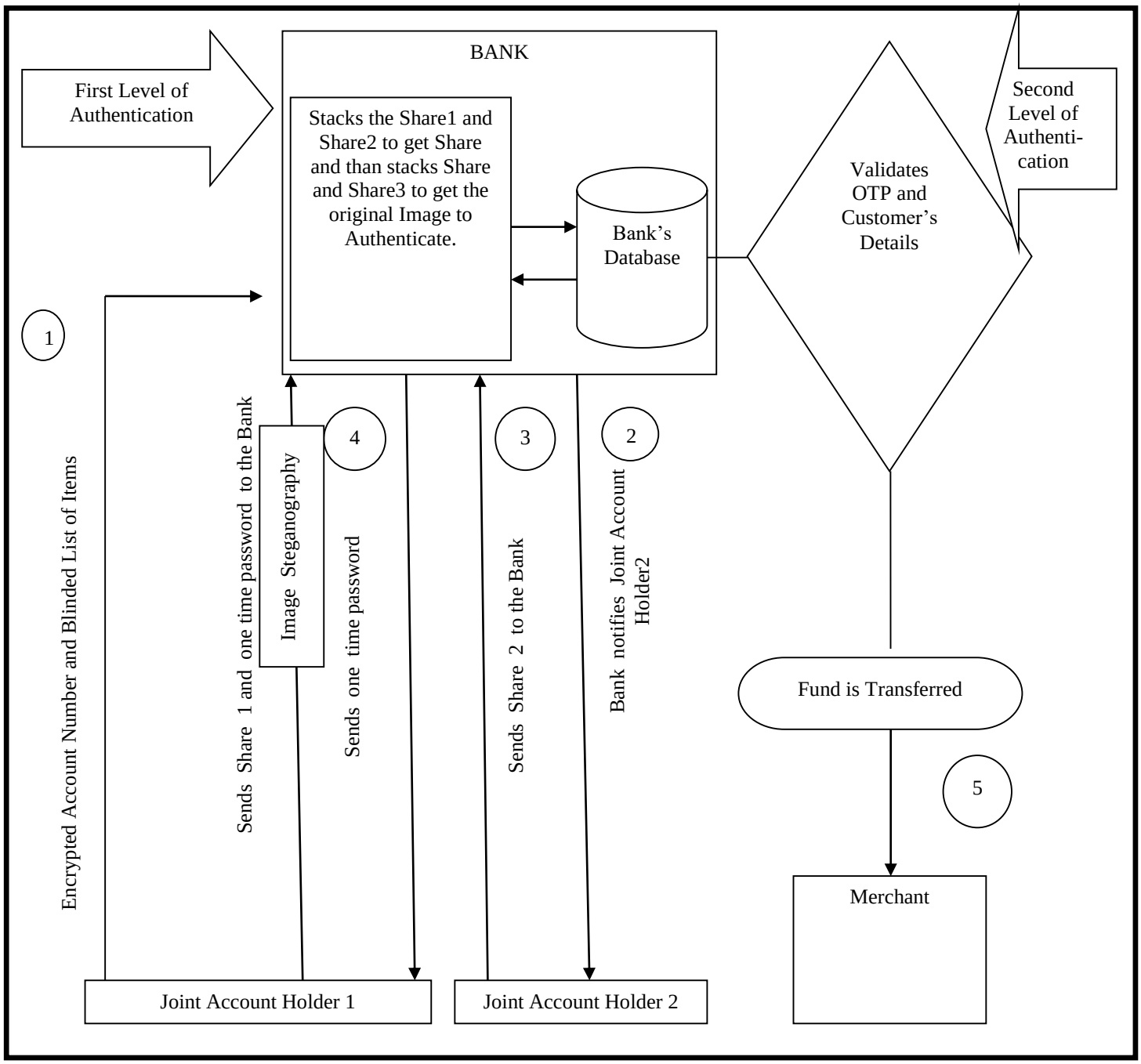
III. INFRASTRUCTURE OF THE PROPOSED SYSTEM

We proposed a new scheme called secure online transaction in the Bank for the maximum security performance. So In proposed online transaction scheme will share minimum information to the merchant. The proposed scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.
Customers can open joint account with bank and can operate jointly or individually. Sometimes joint account holders may be antagonist and one of them may try to cheat other one by withdrawing all the money of performing illegitimate online banking transaction.
The proposed scheme ensures that any type of online banking transaction is possible only when both the joint account holders are aware. It safeguards from any kind of malicious attacks, like phishing, identity theft etc. The attackers do not have any clue as the shares are random noise like images and distributed among three parties so It ensures that nobody can misuse the information stored in the database even they apply as much amount of computing power and time. In the proposed method gray images of both the user are taken as input and processed for further use. Proposed system uses visual cryptography with steganography for image encryption. Both the joint account holders are provided with the private keys.
The proposed method includes four main parties for online transactions: two joint account holders, bank, merchant or retailer. Before purchasing online, the joint account holders must open a bank account by providing their personal details to the bank. When joint account holders open account in the bank, the combined picture of both the joint account holders is taken and scanned and stored in the bank's database.
The combined picture of both joint account holders are broken into two shares. One share is stored in the banks database and other share is further broken into two shares and each share is given to the respective joint account holders.

At the time of online banking transaction

- On receiving blinded list of items along with encrypted account number by the first joint account holder, the second joint account holder is intimated by the bank about the online transaction initiated by the first joint account holder.
- If second joint account holder agrees than he send his share to the bank using for secure transmission as a proof of his consent.
- Now bank generates an one time password and securely transfers it to joint account holder1.
- After receiving one time password, image steganography is performed by taking customer's share as cover image and hidden information as one time password and stego image is passed to bank. Bank extracts embedded one time password so that share and one time password gets separated.
- Bank stacks the respective shares of both joint account holders and further stacks with its parts and verifies.
- Bank validates OTP and joint account holder's details and fund is transferred to merchant account number.

Figure below illustrates



IV. IMPLEMENTATION AND RESULT DISCUSSION

To achieve the security and take the consent of the other joint account holders in every online banking transaction the use of visual cryptography is done. The shares are distributed among three parties so it is safe from any kind of malicious attack. Whenever one of the joint account holders tries to perform any online banking transaction the other joint account holder is notified and he is prompted to send his share to bank for the approval. The Joint account holder's account number and the one time password is sent by using steganography so it is secure and the OTP sent by bank is sent to the customer. The system provides multiple level of authentication This would allow customers to be directly involved in the payment to be made from the customer's bank account and would be done with their approval.

V. MERITS OF PROPOSED SYSTEM

- The proposed system provides multiple level of security by using two levels of shares creation.
- Number of attacks to steal is impossible The total number of attacks to completely impersonate someone is made undefined. It is because, the shares are distributed in three parties and are only known to the clients. Even if the attacker steals one of the security image it will be useless for him, as images are distributed among three parties and during transmission image steganography is used to encrypt the image.
- Multi-step heuristic based technique The heuristics of verifying if the website is not a phishing site is increased by 'Visual cryptography' technique over the security image that is encoded by the account number within a image through 'Steganography'.
- The joint account holders have full control on the online transactions.

VI. CONCLUSION

The visual cryptography and steganography along with RSA algorithm is a secret sharing scheme. In this method original imaged is secured by decomposing into n schemes. This paper proposed for better security provided to phishing attacks, identity theft and customers data in the joint account transaction. For secure banking transaction in joint account operation this paper proposed better way to secure banking transaction visual cryptography method and steganography along with RSA algorithm.

VII. REFERENCES

1. Aaditya Jain, Sourabh Soni, ―Visual Cryptography and Image Processing Based Approach for Secure Transactions in Banking Sector || 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) 2017.
2. Shemin P A, Prof. Vipin kumar K S – E Payment system Using Visual and Quantum Cryptography || International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015)
3. Sayali Vaidya, Shreya Zarkar , Prof. Achal N. Bharambe, Arifa Tadvi,Tanashree Chavan -- Anti-Phishing Structure Based On Visual Cryptography and RSA Algorithm || International Journal of Engineering Trends and Technology (IJETT, 2015)
4. Aparnaa. K. S., Sathyasundaram. M., Santhi. P. -- Securing Internet Banking with a Two – Shares Visual Cryptography Secret Image || International Journal of Engineering Research & Technology (IJERT 2016)
5. B.Srikanth, G.Padmaja -- Secured Bank Authentication using Image Processing and Visual Cryptography || International Journal of Computer Science and Information technology (IJCSIT 2014)
6. Naveen Kumar Kolli -- Implementation of secure payment transaction using AES encryption with extended visual cryptography || (tamucc.edu 2017)
7. Sarita swami, Reshma gulwani -- Secure E-PAY Using Steganogrphy and Visual Cryptography || WRFER International Conference, 2017
8. Dr.S.Makbul Hussain G. Mahaboob Basha -- Online Payment System using Steganography and Visual Cryptography || International Journal & Magazine of Engineering, Technology, Management and Research (www.ijmetmr.com, 2017)
10 Ms. Shital B Patel & Dr. Vinod L Desai -- Cheating Prevention in E-payment System using Visual Cryptography || International Journal of Research and Analytical Reviews (ijrar.com, 2018)
11. John Blesswin A, Christhu Raj, Rajeev Sukumaran & Selva Mary G -- Enhanced semantic visual secret sharing scheme for the secure image communication || (link.springer.com, 2019)
12. Sejal krishna Gajbhiye, Pooja Gedam, Lavanya Gannamani, Mrunal Deshmukh Mobile Banking App Using Visual Cryptograpy And Steganography International Journal of Scientific Development and Research (IJSDR) || (www.ijsdr.org, 2020)