International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 09 | September - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Online Payment Secure System Using Visual Cryptography

Ankita Ajay Wani[1], Dinesh D Patil[2], Yogesh S Patil[3]

[1]Computer Science and Engineering, Sant Gadge Baba College of Engineering and Technology, Bhusawal
[2]Computer Science and Engineering, Sant Gadge Baba College of Engineering and Technology, Bhusawal
[1]Computer Science and Engineering, Sant Gadge Baba College of Engineering and Technology, Bhusawal

---

Abstract - In recent years the growth of the E-Payment system has increased tremendously due to widespread use of internet based shopping and internet based payments. An electronic payment system facilitates the acceptance of electronic payment for offline transfer. An e-Payment system is a way of making transactions or paying for goods and services through electronic means. E-Payment systems are now widely used in all sectors like banking, finance, E-shopping and many more. In the traditional E-Payment systems there were some security threats such as debit, credit card fraud, phishing etc. So to overcome this problem we have introduced an E-payment system which uses visual and quantum cryptographic techniques together for secure transmission. Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of the one-time password. For the OTP processing, we tuned our system with the E-mail OTP notification technique. Image steganography embeds the share with a one-time password which results in secure transmission of the share to bank. The system proposed guarantees unconditional security than traditional E-payment system

***Key Words*:** Image Processing, One-Time password, Online shopping payment, Image encryption pixel value, Quantum Cryptography, Visual Cryptography.

1.INTRODUCTION

This E-shopping refers to process of buying commodities through web browser instead of using mortar stores. Due to wide variety of selection and higher convenience customers are magnetized to E shopping. Even though customer focuses on E- shopping than traditional shopping because of its advantage, security problems such as identity theft and phishing are the major concern for both customers and merchant. Identity theft is the practice of stealing another person's identity for gaining access to his resource whereas phishing refers to the process of acquiring sensitive information by masquerading as a reputed entity [10].

2. LITERATURE SURVEY

Trihastuti Yuniati [1] as This Visual cryptography is a secret sharing scheme where it is an encryption technique to hide information in an image in such a way that it can be decrypted by superimposing two or more shares. Share is a random pixel image generated using visual cryptography algorithm. Visual cryptography produces two shares of the same image, one image contains random pixels and the other contains secret information. No share leads to the original image pixel because every time random pixel is encrypted to create a secret image. When the two shares are superimposed on each other, the value of the original pixel can be determined. Phishing and identity theft are the online shopping's common threats. Phishing is a method of stealing personal confidential information from victims. Victims are tricked into providing their credential by a combination of spoofing techniques. A number of solutions have been proposed in past to prevent this problem, but they are still not effective enough to stop the problem from happening.

Bogdan Bodea [2] as Visual cryptography uses an encryption method that, introduces a surplus of information to hide the message. The image is processed pixel by pixel, taking into account the chosen encryption method and the number of sheets that will be generated. An information matrix of N elements is used to retain the information.

Richa Maurya [3] as This is important to secure the data transmitted in this medium. The shared data could be in the forms of image, audio, video, etc. To provide secrecy of data many techniques have been proposed in the literature review. Visual cryptography is one among them. This paper proposes an Extended Visual Cryptography Technique (EVCT) for medical image security. Visual cryptography is a technique of sharing secret information in forms like images, text, etc. The secret image can be reconstructed without any complex computation. Meaningless shares are used in the visual cryptography technique (VCT) and these shares are not able to avoid the suspicion of attackers. So the extended visual cryptography technique (EVCT) comes into the picture with meaningful shares. The transmission media can be unreliable. Hence cryptography techniques are used for securing the transmitted data. In cryptography, the plain-text is converted into cipher text using a key in the encryption process (at the sender's side). At the receiver end, the cipher-text is converted into plain-text using a key through the decryption process.

Mr. R. Vinothkanna [4] as work concentrates on the secured transmission of the image of multiple formats, by hiding them under a cover image. So the paper incorporates the cryptography into the steganography to enhance the capacity, security and the robustness of the information transfer. The steganography is viewed as the art and the science for maintaining the secrecy in the transmitted information. [4]. There are steganography's available in all file (text, image, audio and video) formats. some of the well-known steganography are that are predominant in maintaining the secrecy of the messages are the least significant bit, linear feedback shift register, DCT, DWT, CWT etc.

Allu Supraja [6] as Visual cryptography (VC) is an emerging area used for data hiding, authentication, multimedia security and transmission of data. Parameters mainly focused in VC are pixel expansion, number of frames, type of images and number of undisclosed message images. Recent research shows many applications uses visual cryptography concept in authentication, secure transaction, secret sharing of information. But visual cryptography shows limited security for VC shares results in lack of security measure. In this paper work different VC (K, N) secret sharing techniques discussed and following analysis shows hybrid approach algorithms used in recent years that can be used for various applications in further implementation with high confidential secret sharing of data.

Singh, Vineet Kumar [7] as he proposed a lossless encryption and decryption algorithm that is applicable in the medical image. Medical images contain information and characteristics related to disease and patient that need lossless image transmission for accurate diagnosis. This algorithm performs encryption process using Circular Bit Shift using group modulo operation. Circular bit shift process applied on pixel bit values of an image to create a new pixel bit value of encrypted image by using group modulo operation. In this algorithm the initial value that associated with Group modulo operation plays an important role as a key value. This algorithm is lossless technique to recover the encrypted image successfully without any loss of data or information. This technique is also applicable in multimedia applications for image, data or information transmission.

defined. Do not use abbreviations in the title or heads unless they are unavoidable.

3. METHODOLOGY

Server will generate snapshot of text containing customer's account number and debit and credit card information is taken. From the snapshot image two shares are generated using visual cryptography. One share will be in the hand of customer and other one will be in database of bank. Merchant and customer agree on a sessional key at the start of E-shopping. After that customer selects the desired items and transfer blinded list of items along with encrypted account number to bank. This blinded list is generated by encrypting list of items with sessional key between customer and merchant. On receiving blinded list of items along with encrypted account number bank generates a one-time password and securely transfers it to customer using quantum cryptography. 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 steno image is passed to bank. Bank extracts embedded one-time password so that share and one-time password gets separated

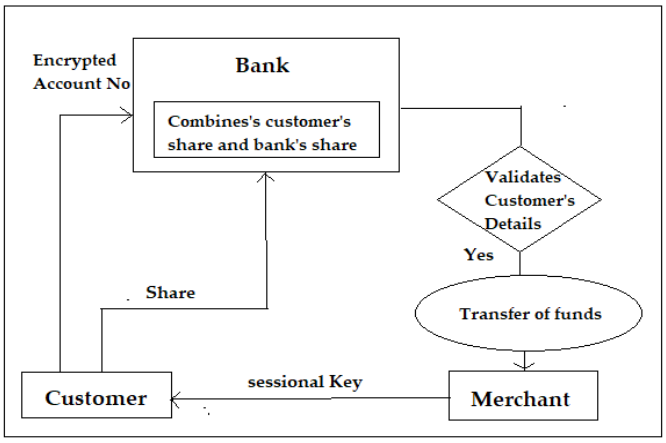


Fig -1: System Architecture Diagram

Then Bank combines customer's share with bank's share and obtains account number and credit card details. Finally, bank validates the one-time password and credit card details and if both verification gets right fund is transferred to merchant account number.

E-payment that provides unrivalled security by using cryptographic techniques like visual cryptography, quantum cryptography and steganography. Visual cryptography hides the authentication details of customer by generating two shares for customer and bank respectively. Quantum cryptography secures the transmission of one-time password. Steganography is used to combine the customer's share along with one-time password in order to secure the transmission of customer's share to bank. Proposed method for E-shopping can be extended for other bank applications.

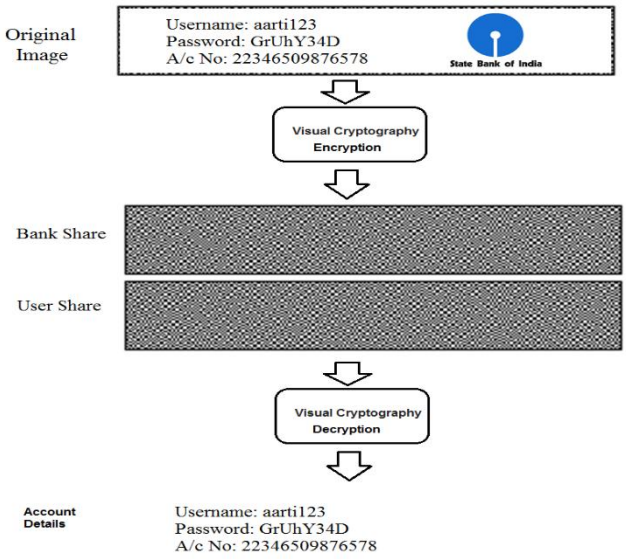


Fig -2: System work flow

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Plaintext is as an image. Encryption involves creating "shares" of the image which in a sense will be a piece of the image.

Give the shares to the respective holders. Decryption involves bringing together the appropriate combination and the human visual system. So basically it involves dividing the image into two parts:

1. Key: a transparency
2. Cipher: a printed page

Secret Sharing refers to a method of sharing a secret to a group of participates. This provides transparency to each one of the n users. Any k of them can see the secret by stacking their transparencies, but any k-1 of them gains no information about it. Main result of the paper includes practical implementations for small values of k and n. [9].

a. ***Encoding the pixels***:

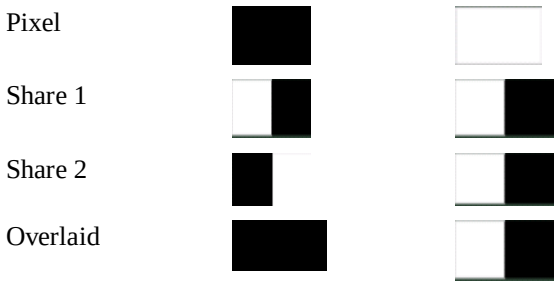


Fig -2: Pixel Encoding

b. Out of 2 Scheme (1 Sub-pixels):

Each pixel is divided in 2 sub pixels i.e. Black and White. For converting the 2x2 pixels matrix chooses the next pixels like if the original pixel is white then randomly choose one of the two rows for white. If it is black, then randomly choose between one of the two rows for black.

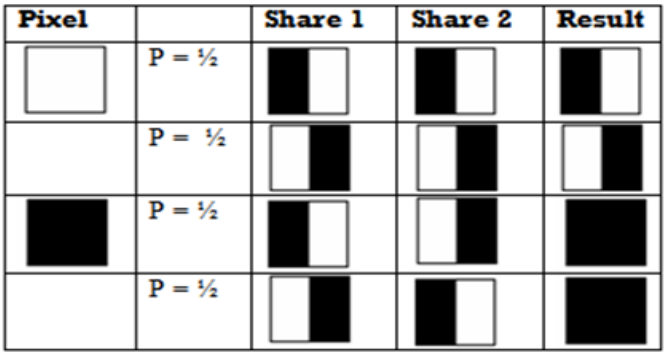


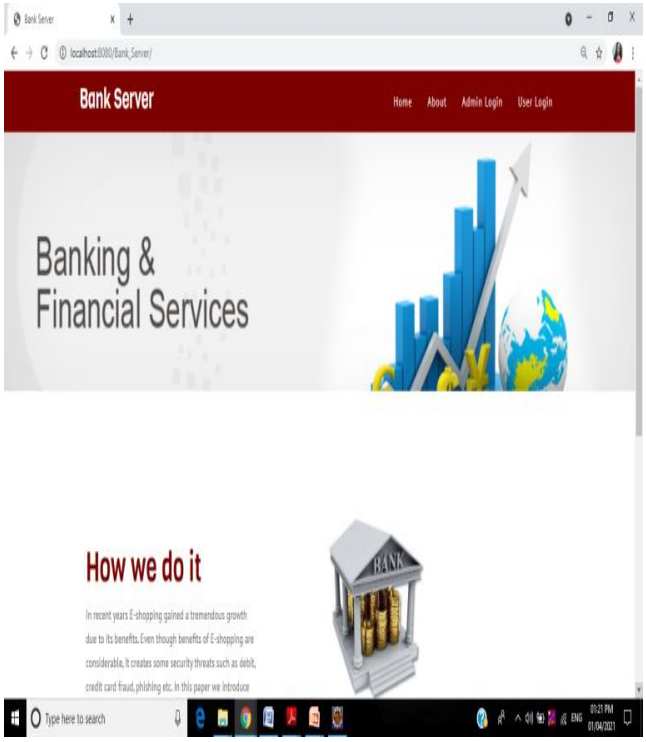
Fig -2: Generation of one share by combination

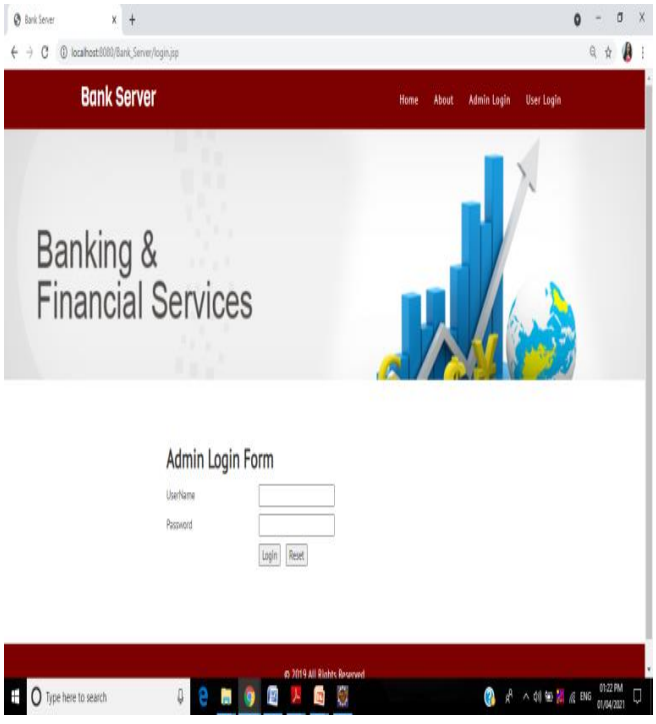
$$C_0 = \left\{ \begin{bmatrix} 0101 \\ 0101 \end{bmatrix} \begin{bmatrix} 1010 \\ 1010 \end{bmatrix} \begin{bmatrix} 0011 \\ 0011 \end{bmatrix} \begin{bmatrix} 1100 \\ 1100 \end{bmatrix} \begin{bmatrix} 0110 \\ 0110 \end{bmatrix} \begin{bmatrix} 1001 \\ 1001 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 0101 \\ 1010 \end{bmatrix} \begin{bmatrix} 1010 \\ 0101 \end{bmatrix} \begin{bmatrix} 0011 \\ 1100 \end{bmatrix} \begin{bmatrix} 1100 \\ 0011 \end{bmatrix} \begin{bmatrix} 0110 \\ 1001 \end{bmatrix} \begin{bmatrix} 1001 \\ 0110 \end{bmatrix} \right\}$$

3. RESULT

Application is developed in Eclipse using Java language, in windows forms template. The developed application is made modularly respecting the principles of programming engineering [5] and has an educational character in the field of cryptography based on visual perception. Figure below shows the start window of the application





Application is easy to use, because as you advance, the available options appear, and in this way the user does not have to know in advance how it works.

4. CONCLUSION

In this paper E-payment we used a method for secure e-Payment transactions using quantum cryptography, visual cryptography and image stenography. This proposed system which is based on two cryptographic techniques provides unconditional security by preventing man in the middle attack. Visual cryptography used in this system safeguards the customer's data whereas quantum cryptography and image steganography prevents security threats such as phishing, identity theft. Proposed method for E- Payment system can be extended for E-shopping, finance sector and bank applications as well. We can also extend the system by providing two factor authentication by providing messaging OTP facilities.

REFERENCES

1. Trihastuti Yuniati, Rinaldi Munir, "Security E-payment method using visual cryptography", 2018.

2. PetreAnghelescu, Ionela-Mariana Ionescu, Marian Bogdan Bodea, "Design and implementation of visual cryptography", 2020.

3. Richa Maurya, Ashwani Kumar Kannojiya, Rajitha B, "An Extended visual cryptography technique for medical image security",2020.

4. Vinothkanna, M. R. (2019). A Secure Steganography Creation Algorithm for Multiple File Formats. Journal of Innovative Image Processing (JIIP), 1(01), 20-30.

5. G. C. Stănică and P. Anghelescu, "Management software for a publishing company", 11th International Conference on Electronics, Computers and Artificial Intelligence, pp. 1-4, 2019, DOI:10.1109/ECAI46879.2019.9042014.

6. Supraja, Allu, and Kakelli Anil Kumar. "Analysis on Hybrid Approach for (K, N) Secret Sharing in Visual Cryptography." 2019 International Conference on Data Science and Communication (IconDSC). IEEE, 2019.

7. Singh, Vineet Kumar, Piyush Kumar Singh, and K. N. Rai. "Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.

8. N. Chaudari and P. Parate, "Secure Online Payment System using Visual Cryptography", in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2016.

9. N.R. Jain, K. Ujwal, S. Apsara, P. Nikhil, and D. Tejashri, "Advance Phising Detection using Visual Cryptography and One Time Password", in International Journal of Advanced Research in Science, Engineering and Technology, Vol. 3, Issue. 4, April 2016.

10. E –payment system using visual and quantum cryptography shemin p a , vipinkumar k s b

11. https://www.kaspersky.com/resourcecenter/definitions/what-is-cryptography

12. https://www.ukessays.com/essays/computerscience/steganography-uses-methods-tools-3250.php

13. https://link.springer.com/chapter/10.1007/978-981-13-8289-5_2

14. https://blog.eccouncil.org/what-is-steganography-and-what-are-its-popular-techniques/

15. https://www.sciencedirect.com/topics/engineering/steganography

16. https://sectigostore.com/blog/what-is-the-difference-between-steganography-vs-cryptography/