

# Using Visual Cryptography, A Safe Online Payment Method

Nagendra R<sup>1</sup>, Bhagyashree K<sup>2</sup>, Pulukuri Aparna K<sup>3</sup>

<sup>1</sup>Computer Science and Engineering, Brindavan College of Engineering and Technology, Bangalore

<sup>2</sup>Computer Science and Engineering, Brindavan College of Engineering and Technology, Bangalore <sup>3</sup>Computer Science and Engineering, Brindavan College of Engineering and Technology, Bangalore

\*\*\*

**Abstract** - Due to the growing usage of online shopping and online payments in recent years, the E-Payment system has experienced enormous growth. The acceptance of electronic payments for offline transfers is made easier by an electronic payment system. An electronic payment system is a technique to conduct transactions or pay for goods and services online. Systems for electronic payments are now widely employed across all industries, including banking, finance, online commerce, and many more. There were some security risks in the conventional e-payment systems, including phishing, credit card fraud, and debit card fraud. In order to solve this issue, we developed an electronic payment system that combines visual and quantum cryptography methods for safe transmission. Quantum cryptography secures the transmission of the one-time password, whereas visual cryptography conceals customer information by creating shares. We adjusted our system using the email OTP notification mechanism for OTP processing. The share is securely transmitted to the bank thanks to image steganography, which embeds a one-time password in the share. The proposed approach offers unconditional security as opposed to the conventional E-payment mechanism.

**Key Words:** One-time passwords, online payments, image processing Quantum cryptography, visual cryptography, and image encryption.

## 1. INTRODUCTION

E-shopping is the practice of purchasing goods through a computer browser as opposed to traditional brick and mortar establishments. Customers are drawn to online buying because of the huge variety of options and higher level of ease. Due to its advantages, customers prefer online shopping over traditional shopping, but security issues like identity theft and phishing are what both customers and retailers are most concerned about. While phishing refers to the activity of obtaining sensitive information by impersonating a reputable company, identity theft is the practice of using another person's identity to access his resources.

## A SURVEY OF THE BOOKS

Trihastuti Yuniati [1] like This Visual cryptography is a type of secret sharing where information is encrypted and concealed in images so that it can be decoded by superimposing two or more shares. The visual cryptography algorithm was used to create the random pixel image known as Share. Using visual cryptography, two copies of the same image are created, one

Random pixels make up one image, while secret information is found in the otherlike This Where it is, visual cryptography is a secret sharing mechanism. Since each random picture pixel is encrypted to produce a hidden image, no sharing goes to the original image pixel. The value of the original pixel can be ascertained by superimposing the two shares. The most frequent dangers to internet buying are phishing and identity theft. Phishing is a technique for stealing from victims' personal information. With the help of several spoofing techniques, victims are coerced into revealing their credential. Numerous remedies to this issue have been put out in the past, yet they are still insufficient to prevent the issue from occurring.

Bogdan Bodea [2] Visual cryptography hides the message by using an encryption technique that adds an excess of information. Pixel by pixel, the image is processed while accounting for the encryption method of choice and the quantity of sheets that will be produced. The information is stored in a N element information matrix.

Richa Maurya [3] Assuring the security of data carried over this medium is crucial. The exchanged data may take the shape of a picture, audio file, or video, for example. Numerous strategies have been suggested in the literature review to ensure data secrecy. One of them is visual cryptography. In this research, an Extended Visual Cryptography Technique (EVCT) for the security of medical images is proposed. Visual cryptography is a method for transmitting confidential information in formats like text, graphics, etc. Without using any complicated calculations, the hidden image can be recreated. The visual cryptography technique (VCT) employs meaningless shares, however attackers cannot avoid suspicion when using these shares. With substantial shares, the extended visual cryptography technique (EVCT) enters the picture. The transmission medium could not be trustworthy. As a result, the sent data is secured using cryptographic techniques. In cryptography, a key is used throughout the encryption process (at the sender's side) to transform the plain-text into encrypted text. Using a key, the cipher-text is decrypted at the receiving end and then transformed into plain-text.

Mr. R. Vinothkanna [4] since the focus is on securely transmitting images in numerous formats while concealing them with a cover image. In order to increase the capacity, security, and robustness of the information transport, the study integrates cryptography into steganography. Steganography is regarded as the science and art of keeping the transmitted information secret. [4]. All file types, including text, image, audio, and video, support steganography. The least significant bit, linear feedback shift register, DCT, DWT, CWT, and other well-known steganography techniques are some of those that are frequently used to keep communications secret.

Allu Supraja [6] The visual cryptography (VC) is a new field utilized for data transfer, multimedia security, and data transmission and authentication. The parameters that are mostly focused in VC include pixel expansion, frame count, picture kind, and quantity of secret message images. According to recent research, the concept of visual cryptography is used in various applications for authentication, secure transactions, and secret information sharing. But visual cryptography demonstrates that the lack of security measures for VC shares is the outcome of limited security. Different VC (K, N) secret sharing strategies are covered in this paper work, and the analysis that follows demonstrates hybrid approach algorithms that have been employed recently and may be applied to a variety of applications with high confidentiality secret data sharing.

Singh, Vineet Kumar [7] he suggested a lossless encryption and decryption system that can be used with medical images. Lossless image transmission is required for reliable diagnosis of the diseases and patient features contained in medical photographs. This approach uses group modulo operation and circular bit shift to accomplish encryption. In order to construct a new pixel bit value for an encrypted image using group modulo operation, a circular bit shift procedure is used on the image's pixel bit values. The starting value connected to the Group Modulo operation serves as a crucial key value in this algorithm. The encrypted image can be successfully recovered using this procedure without any data or information being lost. This method can also be used in multimedia programs for images, data, or conveyance of information.

Defined. If at all possible, avoid using abbreviations in the title or headings.

## 2. MECHANISMS

The server will produce a text snapshot comprising the account number of the customer as well as their debit and credit card details. Using visual cryptography, two shares are created from the snapshot image. The consumer will hold one share, and the bank's database will hold the other. At the commencement of electronic commerce, the merchant and the client agree on a sessional key. The customer then chooses the desired items and sends a blinded list of them to the bank together with an encrypted account number. This blinded list is created by encrypting the consumer and merchant's sessional key list of products. When a bank receives a blindfolded list of items and an encrypted account number, it immediately produces a one-time password and securely sends it to the consumer. After being given one-time, password, or picture By using the customer's share as the cover image and the concealed information as a one-time password, steganography is carried out, and the bank is then sent the steno image. In order to separate the share and the one-time password, the bank extracts the encoded one-time password.

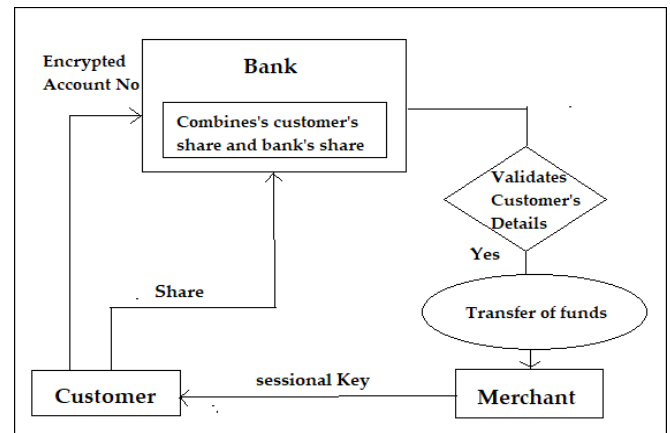


Fig -1: System Architecture Diagram

The bank then combines the client and bank portions to obtain the account number and credit card information. Finally, the bank verifies the credit card information and one-time password, and if both checks are successful, money is transferred to the merchant account number.

E-payment that uses steganography, visual cryptography, and quantum cryptography to achieve the highest level of security possible. By creating two shares for the consumer and the bank, respectively, visual cryptography conceals the customer's authentication information. The transmission of one-time passwords is secure thanks to quantum cryptography. In order to safeguard the transfer of the customer's share to the bank, steganography is employed to combine the customer's share with a one-time password. The suggested approach to online buying can be expanded to other bank applications.

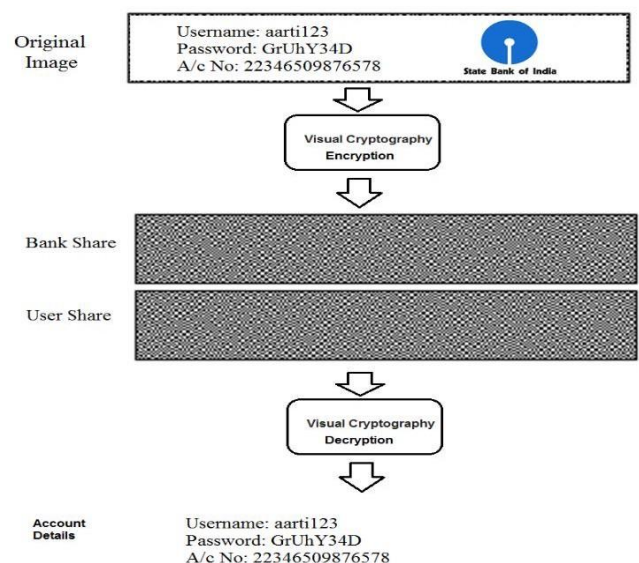


Fig -2: System work flow

Visual cryptography is a cryptographic method that makes it possible to encrypt visual data (images, text, etc.) in a way that makes decryption a mechanical process that does not require a computer. An image of plaintext is used. In order to encrypt an image, "shares" of the image must be created, each of which will represent a portion of the image.

Transfer the shares to the appropriate owners. Combining the right combination with the human visual system is necessary for decryption. In essence, this requires splitting the image into two parts:

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

A way of disclosing a secret to a group of participants is known as "secret sharing." Each of the  $n$  users has transparency thanks to this. By stacking their transparencies, any  $k$  of them can see the secret, but any  $k-1$  of them learns nothing about it. Practical implementations for modest values of  $k$  and  $n$  are the paper's main outcome.

a. **Encoding the pixels:**

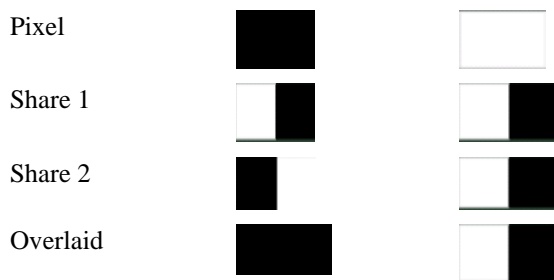


Fig -2: Pixel Encoding

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

Black and White are the two subpixels that make up each pixel. If the original pixel is white, then a random row from the two rows is chosen to be the next pixel to be converted in the 2x2 pixels matrix. If it's black, pick one of the two rows at random for black.

















Pixel		Share 1	Share 2	Result
	$P = \frac{1}{2}$			
	$P = \frac{1}{2}$			
	$P = \frac{1}{2}$			
	$P = \frac{1}{2}$			

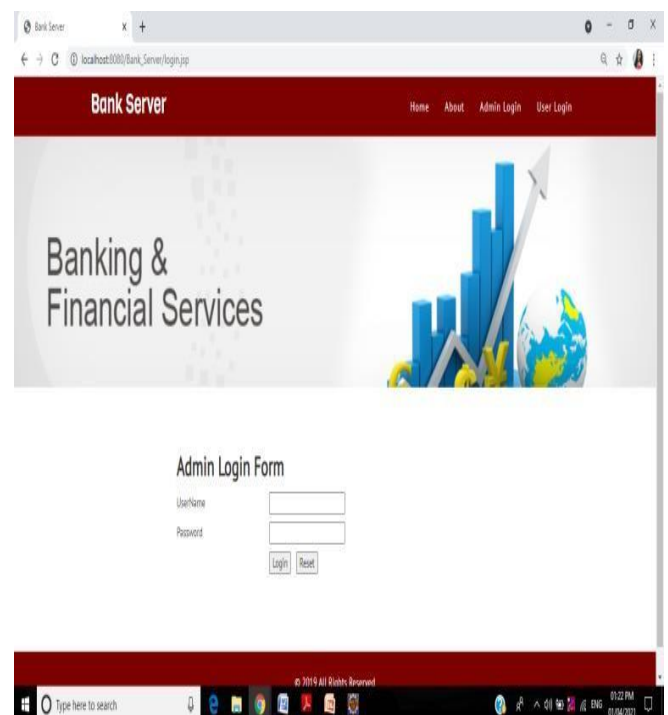
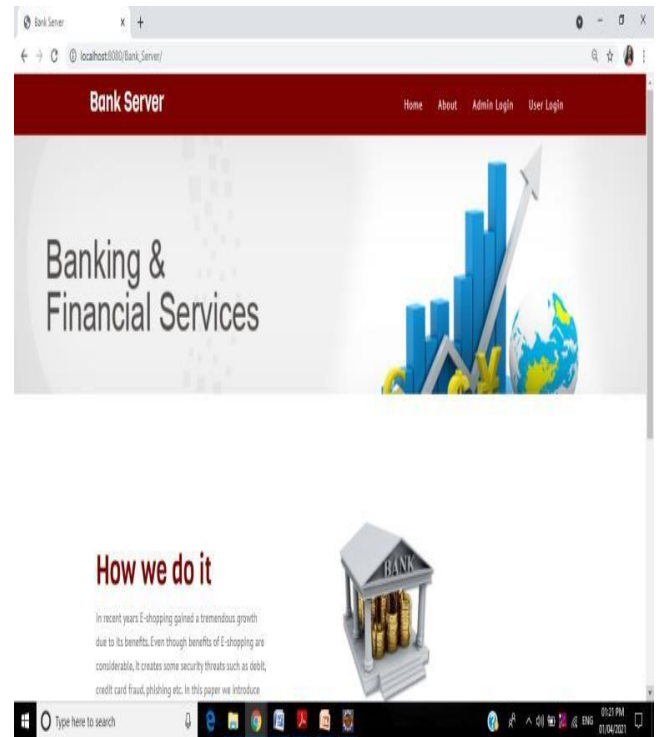
Fig -2: Generation of one share by combination

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

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

### 3.RESULT

Java is used to create the application, which is built using the windows forms template in Eclipse. The created application is constructed in a modular manner while adhering to the fundamentals of programming engineering [5] and contains a teaching component in the area of visual perception-based encryption. The application's start window is depicted in Figure below.



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 study, we present a safe e-payment approach that combines image stenography, visual cryptography, and quantum cryptography. By prohibiting man-in-the-middle attacks, the suggested system, which is based on two cryptographic algorithms, offers absolute security. This system uses visual cryptography to protect consumer data, while quantum cryptography and image steganography mitigate against security risks including phishing and identity theft. The suggested system for electronic payments can be expanded to include applications in the financial sector, banks, and online shopping. Additionally, we may enhance the system by enabling two-factor authentication via messaging OTP facilities.

#### REFERENCES

1. Trihastuti Yuniati, Rinaldi Munir, "Security E-payment method using visual cryptography", 2018.
2. PetreAngheliescu, 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. Angheliescu, "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
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](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/>