IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Implementation of Visual Cryptography in Securing Payments

1.Mr. Vairage Rajkumar Banshidhar 2.Dr B.M.Patil
1.Scholar 2.Project Guide
1.Computer Science and information technology
1.Dr. Babasaheb Ambedkar Technological University

Abstract: In recent years E-shopping gained a tremendous growth due to its benefits. Even thoughbenefits of E-shopping are considerable, it creates some security threats such as debit, credit card fraud, phishing etc. In this paper we introduce an E-payment system that provides an unrivalled security using visual and quantum cryptography. Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of one time password .Image steganography embeds the share with one time password which results in secure transmission of share to bank. Proposed approach guarantees unconditional security than traditional E- payment system by using two important cryptographic techniques.l

Keywords: **visual cryptography, Network Security, Web security**

1.INTRODUCTION

1.1Introduction Visual Cryptography

The word cryptography is derived from two Greek words which mean "secret writing". Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others.

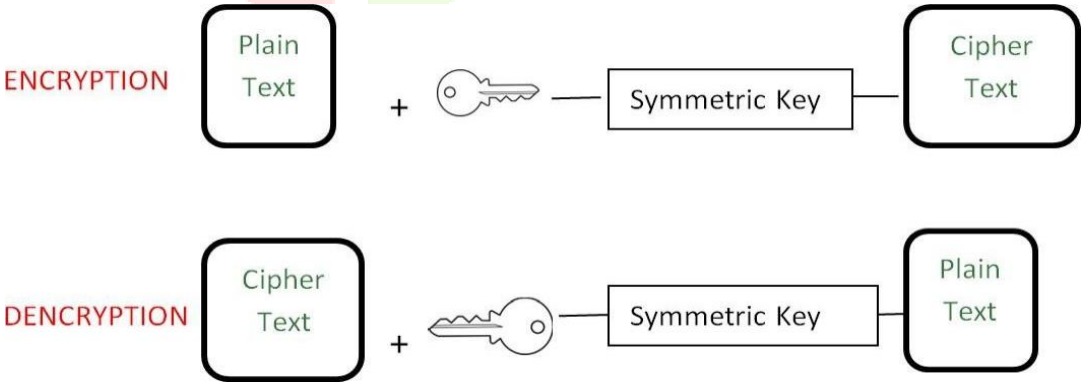


Fig 1.Symmetric key encryption

Cryptography is an effective way to protect the information that is transmitting through the network communication path.

- **What is visual cryptography?**

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be done just by sight reading. Visual cryptography, degree associated rising cryptography technology, uses the characteristics of human vision to rewrite

encrypted photos. Visualcryptography provides secured digital transmission that is used just for merely the once.

Numerous guidance like military maps and business identifications are transmitted over the internet. Whereas pattern secret photos, security problems ought to be compelled to be taken into thought as a result of hackers may utilize weak link over the communication network to steal info that they need.To touch upon the protection problems with secret photos, varied image secret sharing schemes are developed. anyone will use it for coding with none science information and any computations.

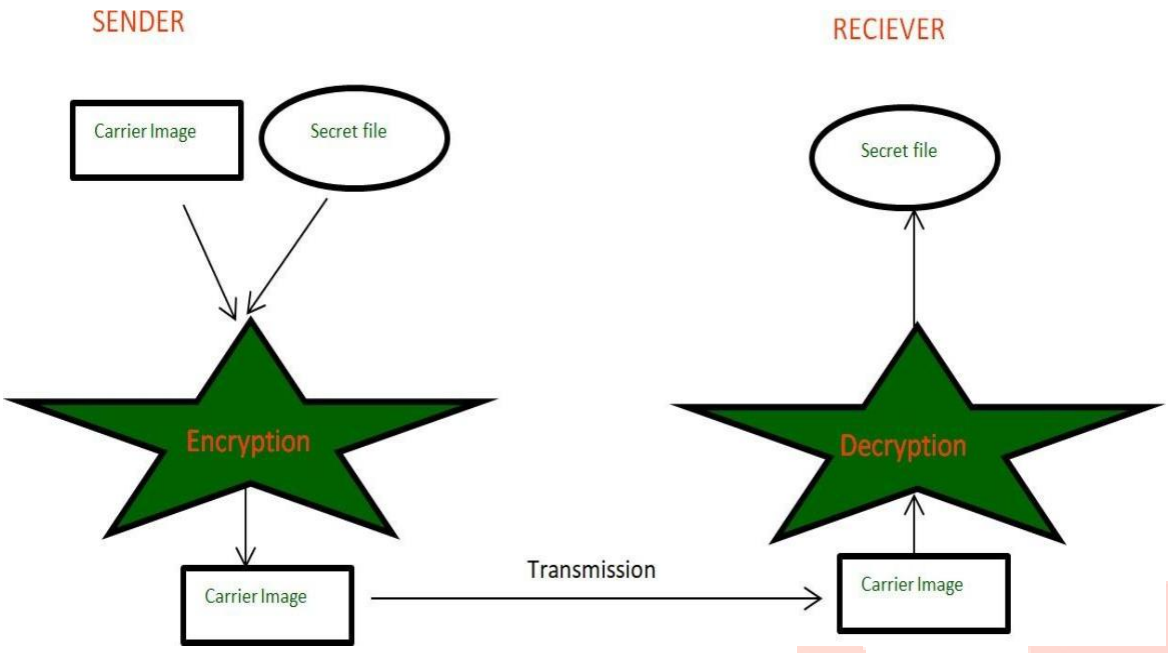


Fig 2.Process of cryptography

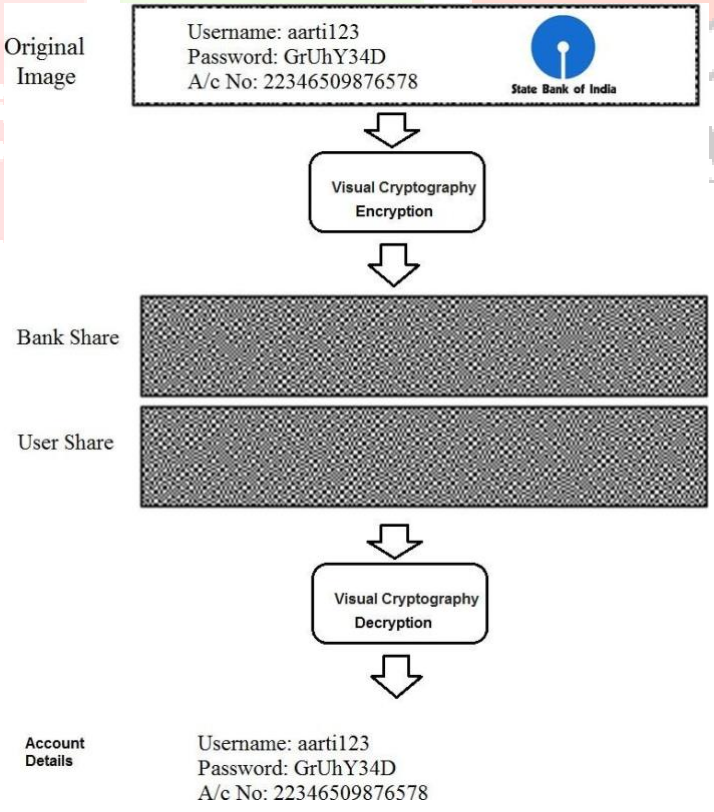
A visual cryptography design is a type of secret image sharing which permits the encoding of a secret image into different shares. The disadvantage of visual cryptography design is that even a normal person is capable to decipher the secret image devoid of having any cryptographic information and computational tools. An embedded image cryptography schemeis a type of image cryptography scheme which consists of significant shares. In this paper, we proposed the method Embedded Visual Cryptography Scheme (EVCS) using gray threshold values with morphological erosion operations for secure transmission of bank cheque over theinternetwork. Initially in this method apply gray threshold values with morphological operationand then split the input original image into diverse number secret share images using conventional visual cryptography system. Implant the each share image into different cover images. Finally, mound the implanted images to get the original information of image. For example, partition the input image into two share images. In that the random pixels in one shares and secret information in other share. In order to get the original image basically overliethe both shares of the images.

VC suggested by Naor and Shamir in 1994 is a type of image cryptography having few computation. It is to make two images derived from original image just by converting each pixel to pattern looking like noise or gray. The images are shared to others. If you again want to catch sight of original image, you gather and stack up the shared images then can see the image. Distinctively it has lower computational cost to encrypt than other cryptography. Decryption method does not even require any computation because it is dependent only on sight of human In order to build the shared images, firstly you should prepare an original imageincluding secret message “0129” such as picture (a) of Figure3. It must be exactly composed of white background and black letter. In fact, the research about VC has been extended to half-tone picture moreover color picture. But we are supposed to explain basic VC referred

to this paper. For encryption, you should prepare some patterns consisted of 4 subpixels arranged ina

2 x 2 array. The half of 4 subpixels is filled with black and the rest becomes transparent. It can make 6 pattern which is horizontal, vertical and diagonal. VC transforms per a pixel of original image to one of those. After VC-based image is made in full, the subpixels become asnoise because shared image is combination of randomly collected patterns. The way to construct pixels of background and message in shared image should be different from each other. If what you want to convert to a pattern is a pixel of background in original image, it should be following to background pixel matrix in Figure4. The pattern is randomly determinedby one of the forms according to pattern no. For example, if you want to convert a pixel of background in original image to pattern no3, subpixels of the position in first shared.

3 We propose a new method for E-payment that provides unrivaled security by using cryptographic techniques 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 forE-shopping can be extended for other bank applications.



2. LITERATURE REVIEW

Up till now more work or research has been done in Epayment security techniques.Lotsof efficient techniques are proposed till.The work done in Epayment security using visual cryptography are as follows:

Epayment Security using Visual Cryptography Techniques

Rajaram et.al [1], It explained that banking system had carried banking for the customer's expediency, supporting set of services, where authentication plays a vital role. Due to the fabulous apprehension and growth in the field of hacking, that it is not safe to rely on web to accumulate all the information. So inorder to beat this problem we have proposed an efficient algorithm for secured bank cheque authentication by embedded image Cryptography scheme. It is a cryptographic approach that uses visual information as input, encryption and decryption is done by using human visual system. The proposed method Embedded Visual Cryptography Scheme (EVCS) uses gray threshold with morphological operation for secure transmission of bank cheque over the network. In this approach first apply gray threshold with morphological operation and divide the input image into different number of secret share images using traditional visual cryptography technique. Embed the each share into different cover images. Finally, stack the embedded images to get the original information of images. The performance of proposed method is calculated by using PSNR, UQI and MSE Value. The proposed EVCS shows the high performance in terms PSNR, UQI and MSE for secure transmission of bank cheque over network.

Yang et.al [2], proposed Traditional password conversion scheme for user authentication was to transform the passwords into hash values. These hash-based password schemes are comparatively simple and fast because those are based on text and famed cryptography. However, those can be exposedto cyber-attacks utilizing password by cracking tool or hash-cracking online sites. Attackers can thoroughly figure out an original password from hash value when that is relatively simple and plain. Asa result, many hacking accidents have been happened predominantly in systems adopting those hash- based schemes. In this work, we suggest enhanced password processing scheme based on image using visual cryptography (VC). Different from the traditional scheme based on hash and text, our scheme transforms a user ID of text type to two images encrypted by VC. The user should make two images consisted of sub pixels by random function with SEED which includes personal information. The serveronly has user's ID and one of the images instead of password. When the user logs in and sends anotherimage, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate user by comparing extracted ID with the saved one. Our proposal has lower computation, prevents cyber-attack aimed at hashcracking, and supports authentication not to expose personal information such as ID to attackers.

Dalvi [3], proposed Security is a vital issue to be taken care of and to be experienced with different perspectives and preventive measures. In the present time, entire web is coming nearer from content information to mixed media information. One of the real security concerns is the insurance of this sight and sound information. Picture, which covers the most noteworthy rate of the media information, its assurance is essential. These might incorporate Military Secrets, Commercial Secrets and Information of people. This can be accomplished by visual Cryptography. It is one sort of picture encryption. In current innovation, the greater part of visual cryptography is implanted a mystery utilizing various shares.

Shemin [5], in this system E-shopping gained a tremendous growth due to its benefits. Even though benefits of E-shopping are considerable, it creates some security threats such as debit, credit card fraud, phishing etc. In this paper we introduce an E-payment system that provides an unrivalled security using visual and quantum cryptography. Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of one time password .Image steganography embeds the share with one time password which results in secure transmission of share to bank. Proposed approach guarantees unconditional security than traditional E-payment system by using two important cryptographic techniques.

Kumar[13], had explained Online payment eco system is the main target especially for cyber frauds. Therefore end to end encryption is very much needed in order to maintain the integrity of secret information related to

transactions carried online. With access to payment related sensitive information, which enables lot of money transactions every day, the payment infrastructure is a major target for hackers. The proposed system highlights, an ideal approach for secure online transaction for fund transfer with a unique combination of visual cryptography and Haar based discrete wavelet transform steganography technique. This combination of data hiding technique reduces the amount of informationshared between consumer and online merchant needed for successful online transaction along with providing enhanced security to customer's account details and thereby increasing customer's confidence preventing "Identity theft" and "Phishing". To evaluate the effectiveness of proposed algorithm Root mean square error, Peak signal to noise ratio have been used as evaluation parameters.

3.METHODOLOGY

3.1 System Architecture

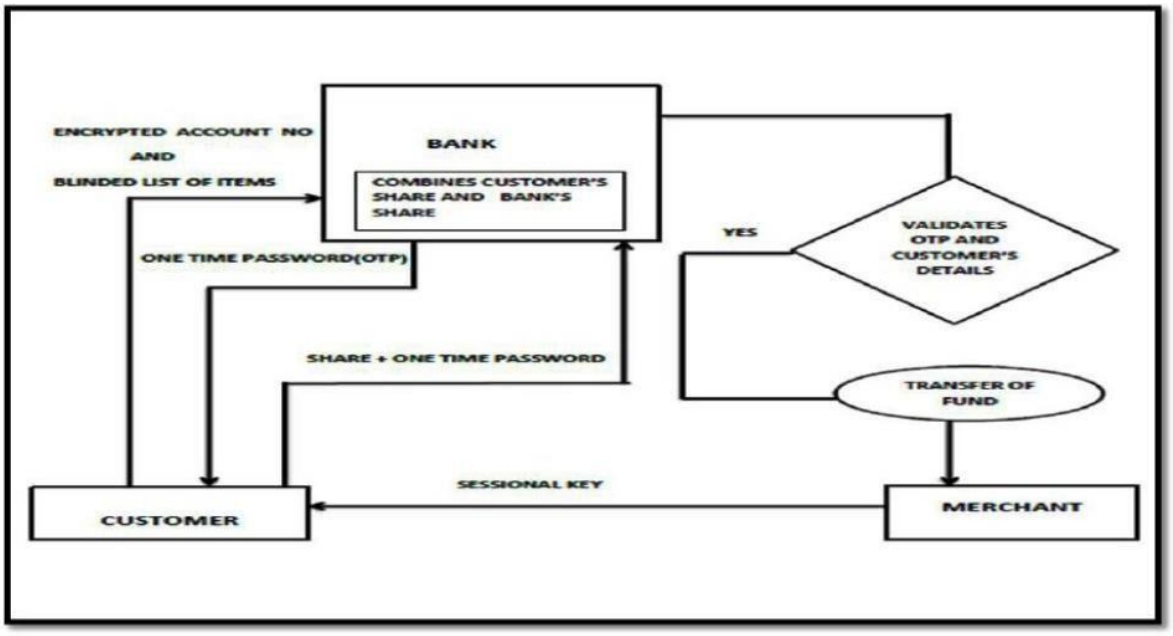


Fig 3.Architecture diagram

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 visualcryptography. One share will be in the hand of customer and other one will be in database of bank. Merchant and customer agrees on a sessional key at the start of E-shopping. After that customer select 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 sessionalkey between customer and merchant. On receiving blinded list of items along with encrypted account number bank generates an 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 stego image is passed to bank. Bank extracts embedded one time password so that share and one time password gets separated. Then Bank combines customer's share with bank's share and obtains account number and credit card details. Finally bank validates the onetime password and credit card details and if both verification gets right fund is transferred to merchant account number.

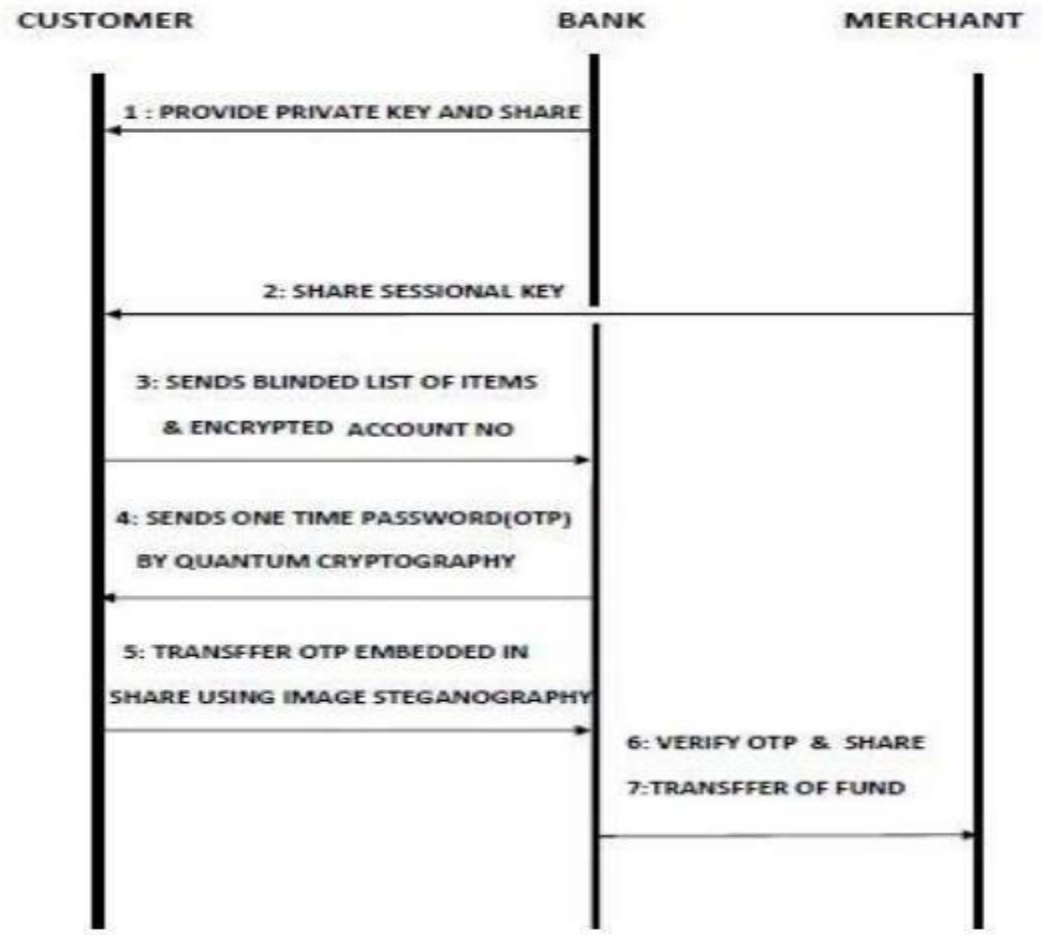


Fig 4.The Security properties of electronic payments adapted from reference

- In proposed method 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 agrees on a sessional key at the start of E-shopping
- Customer do shopping and start for payment
- Bank generates an 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 stego image is passed to bank
- Bank extracts embedded one time password so that share and one time password getsseparated.
- Then Bank combines customer's share with bank's share and obtains account numberand credit card details.
- Finally bank validates the one time password and credit card details and if bothverification gets right fund is transferred to merchant account number.

3.2 Scope

Visual cryptography hides the details of customer by generating shares whereas Quantum cryptography secures the transmission of one time password .Image steganography embeds theshare

with one time password which results in secure transmission of share to bank. Proposedapproach guarantees unconditional security than traditional E-payment system by using two important cryptographic techniques.

3.3 Project Algorithm

Input: Bank details in imageOutput: E-Payment

Steps:

- Create a normal user
- While registration create image which content bank details of new user
- Break that image into 2 shares using visual cryptography
- Mail one share to user
- Add second image to database and link that image with new user
- Create merchant user
- Now do shopping
- View your cart and checkout
- Upload your share to shopping site
- That share will come to bank site with your userid
- Bank Server will match the share with that user and extract the banking details
- If all details are correct and users has sufficient balance, then do the transaction
  - Else report problem to user

Stop

3.4 Feasibility Study Of Project0

1. Visual cryptography:

- Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appearsas a visual image. An image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about theoriginal image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all *n* shares were overlaid, the original image would appear. There extract the banking details
- If all details are correct and users has sufficient balance, then do the transaction
- Else report problem to user

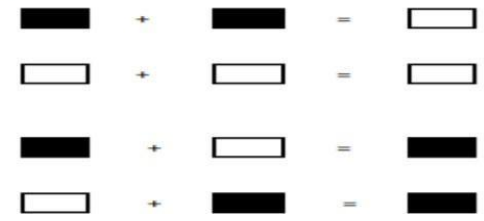
Stop

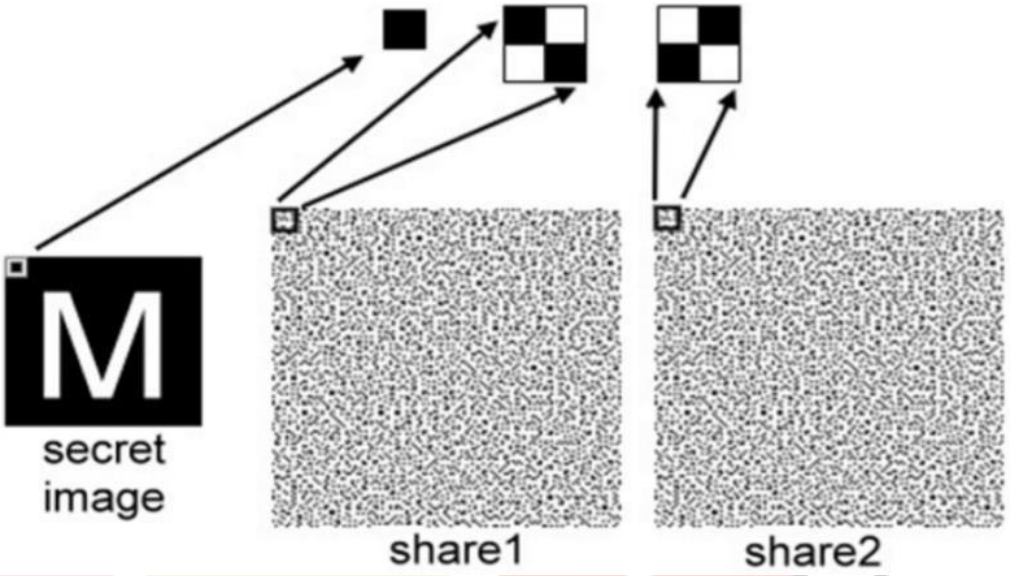
Algorithm Used:

2. Visual cryptography:

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image. An image wasbroken up into n shares so that only someone with all n shares could decrypt the image, while any n −1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all *n* shares were overlaid,the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

Step 1: Generate R1 as a random grid.
Step 2: for (each pixel R1 [x, y], 1 x w and
1 y h) do
Step 3: R1 [x, y] = randpixel(0, 1)
Step4 : for(eachpixelB[x, y], 1xwand1yh)do Step5
if(B[x, y] = 0)R2[x, y] = R1[x,
y]elseR2[x, y] = R1[x, y] .
Step6 : output(R1, R2).





3. Steganography:

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. The word steganography is derived from the Greek words steganos (meaninghidden or covered) and the Greek root graph (meaning to write). Steganography canbe used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content.

Encoding Steps:

1. Take input from user in the text form.
2. Each letter is represented by its ASCII code.
3. The ASCII code will be represented in 8 bit binary number.
4. This 8 bit number is further divided into two parts 4 bit each.
5. 5 Every part of this number will be assigned with 0 to F hex code. Then further this will be used to select the corresponding suitable words in the table shown below:

E-Payment Using Visual Cryptopgraphy: Given a failure case viz. Q, Invalid imageselection & image get distorted; we devise an algorithm for this problem as follows:

For a Problem P1 to be NP-Hard, Satisfiability problem (SAT) must be reducible to P1;SAT ≤ P ;

Let the propositional formula be: G = X1^X2Where

X1: True if Invalid image selectionX2: True

if image get distorted

Algo sati()
{
For i: 1 to 2

x_i = Choice(True,False);if G(x_1,x_2)

then

Success();else

failure();

}

Therefore, since the problem becomes a decision problem, it is **NP.**

- ***Satisfiability and Reducibility:***

3 SAT problem is NP Complete. The system can be reduced to 3SAT problem. A 3SAT problem takes a Boolean formula S that is in CNF in which each clause has exactly three literals. 3SAT is a restricted form of CNF-SAT problem.

x_1 – Image Capturing Modulex_2 - Crate
Shares Module
x_3 – OCR

S = (x_1 ^ x_2 ^ x_3)Algo sat()
{
For i= 1 to 3 X_i=Choice(true,
false)If($S_{(x1,x2,x3)}$= true)
Success()Else
Failure()
}
As it is polynomial time. It is NP-Complete.

4.RESULT AND DISCUSSION

4.1 Result Analysis

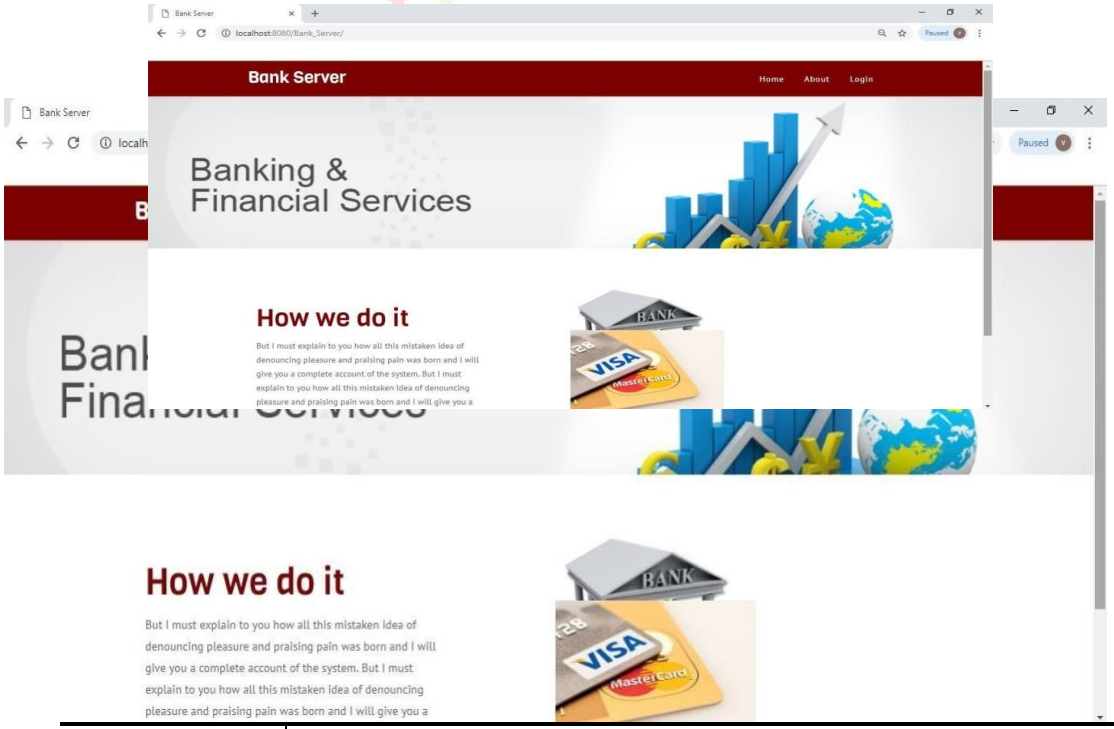
The Combined approach of Text steganography and RG-visual cryptography with CA will ensure end user with information privacy and protect data from being misused. Hence by usingthis combined approach in our proposed payment system, it has been proved secure and protects customer's payment details being hacked by network intruders or attackers. This technique results in more time utilization as it must encrypt and decrypt the greater number ofpixels. Also transferring this high memory pixels through network is also time consuming.

When all n shares are superimposed, the probability of black spots appearing on white pixels in the secret image is (i+1)/(n+i) while the black pixels are fully black (100% black). After superimposing all the shares, the black-and-white contrast is (n-1)/(n+i), where i=2, 3, ..., and n, Therefore, the black-and-white contrast in the superimposed image is larger when i is smaller, which leads to a better quality of the restored secret image

Table 4.1 Table Result Analysis

Authors	Share (Shadow Image)				Restored Image	
	Size	Content	Contrast	Leakage Of Secret	Contrast	Quality
Fang & Lin	2 x 2	Noise-like	-	Yes	50%	Poor
Fang	2 x 2	Meaningful	25%	Yes	50%	Poor
Our Method	2 x 2	Meaningful	(il)/(n+i)	No	(n1)/(n+1)	Good

fig 5.Screenshots of proposed model



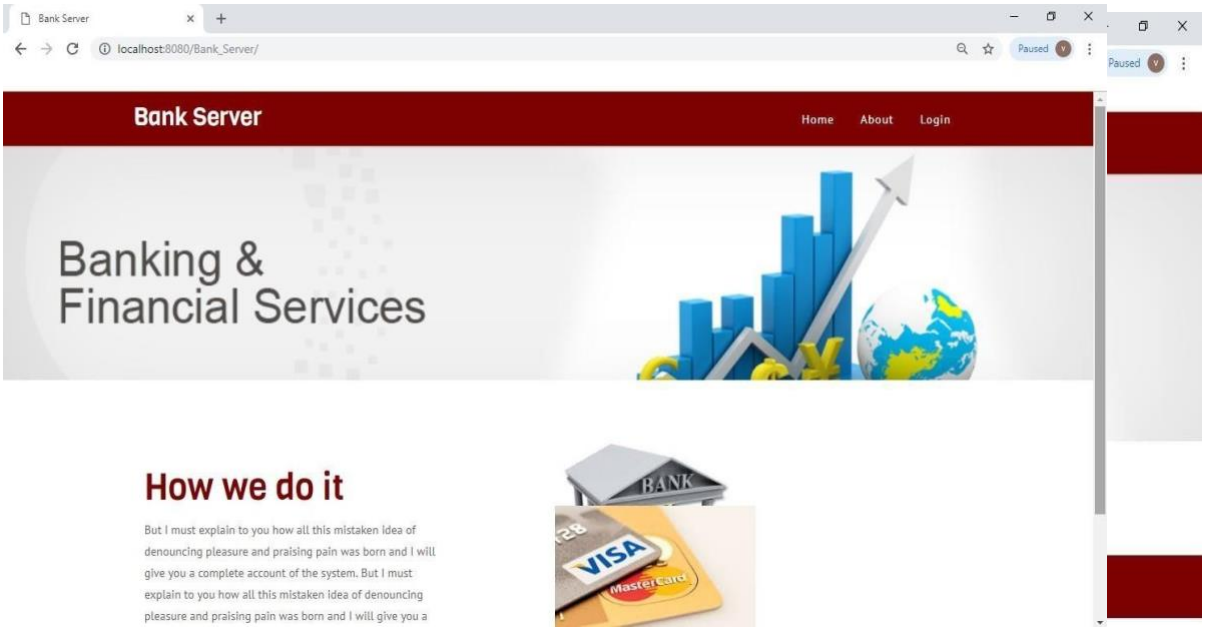


Fig 5 .Screenshot of Login Page

5.Conclusion

The proposed method preserves secret information of users, Verifies whether the website is a genuine/secure website or a phishing website. In this way project helps user to pay securly.
e watermarked halftone image

4.2 Future Scope

Visual cryptography is the current area of research where lot of future scope exists. Rightnow, different cryptographic techniques are is being used by several countries for secretly transfer of handwritten documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. Visual cryptographic work can be extended with the format of color images, three dimensional Images, better quality color images, a greater number of shares andmultiple secret images.

- Multi-pixel Encoding with Variable Block Size
  Multi-pixel encoding is an emerging method in visual cryptography for that it can encode more than one pixel for each run. However, its encoding efficiency is still low. The length of encoding at one run is equal to the number of the consecutive same pixels met during .scanningthe secret image.

- Joint Visual Cryptography and Watermarking
  Both halftone watermarking and visual cryptography involve a hidden secret image. However, their concepts are different. For visual cryptography, a set of share binary images is used to protect the content of the hidden image. The hidden image can only be revealed when enough share images are obtained. For watermarking, the hidden image is usually embedded in a single halftone image while preserving the quality of the watermarked halftone image

REFERENCES

[1] Rajaram, R.Suganya, “Embedded Visual Cryptography for Secure Transmission ofBank cheque “,Proceedings of 2017,IEEE International Conference on Circuits. and.Systems (ICC2017)

[2] Yang, Instill Doh and Kijoon Chae, “Enhanced Password Processing Scheme Basedon Visual Cryptography and OCR”, IEEE, 978-1-5090-5124-3/17, 2017.

[3] Gopal D.Dalvi and D.G.Wakde,“Facial Images Authentication In Visual CryptographyUsing Sterilization Algorithm”, IEEE, 978-1-5090-4307-1/17, 2017.

[4] P.A.Shemin and K.S.Vipinkumar, “E –Payment System Using Visual And Quantum Cryptography” Procedia Technology 24, pp.1623 – 1628, 2016.

[5] Petre Anghelescu, Ionela-Mariana Ionescu and Marian Bogdan Bodea “Design and implementation of a visual cryptography application”, IEEE,pp. 9781-7281,2020