SECURE E-PAY USING TEXT BASED STEGANOS AND VISUAL CRYPTOGRAPHY

Mrs.D.MURUGESWARI[1,] KN.SANGEETHA[2], M.SRIVANI[3]

[1]Assistant Professor, Dept of Information Technology, Panimalar Institute of Technology

[2,3]Students, Dept of Information Technology, Panimalar Institute of Technology

deswari01@gmail.com, sangi.vinai@gmail.com, srivani0394@gmail.com

ABSTRACT— A high-speed prosperity in E-Commerce market has been witnessed in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks. The main motive of this project is to provide high level security in E-Commerce applications and online shopping. This project minimizes detailed information sharing between consumer and online merchant but enable successful fund transfer thereby safeguarding consumer information and preventing misuse of information at merchant's side. This is achieved by the introduction of Central Certified Authority (CA) and combined application of Steganography, Visual Cryptography and Digital Signature for this purpose .

KEYWORDS—E-Commerce, Online Shopping, Identity Theft, Phishing, Steganography, Visual Cryptography, Digital Signature

I. INTRODUCTION

Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Identity theft and phishing are the common dangers of online shopping.

Identity theft is the stealing of someone's identity in the form of personal information and misusing that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft. Phishing is an illegitimate mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Service, Financial and Retail Service are the most focused industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others. In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side.

The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking. Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text , image , video , audio are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line , in open spaces , in word sequence . Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication .Visual Cryptography (VC), is a cryptographic technique based on visual secret sharing used for image encryption. The main motive of the proposed system prescribed in this paper is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be done by using combination of two applications: BPCS Steganography and Visual Cryptography for safe online shopping and consumer satisfaction.

The rest of the paper is organized as follows: Section II gives brief description of experimental/ simulation i.e. methodologies, algorithms, architecture, work flow and use case diagrams. Section III contains results/discussions i.e. results of text based steganography and visual cryptography algorithms. Section IV concludes the paper

II. EXPERIMENTAL/ SIMULATION

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing least information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of BPCS Steganography and Visual Cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer.

FEATURES OF PROPOSED SYSTEM

- Proposed method minimizes customer’s detailed information sent to the online merchant. So even if a breach takes place in merchant’s database, customer doesn’t get affected.
- Certified Authority acts as a fourth party thereby enhancing customer’s satisfaction and security further.
- Usage of BPCS Steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy. It provides a higher level of security and a high information hiding capacity.
- Since customer data is distributed over 3 parties, a breach in single database can easily be contented. Linkguard Algorithm is efficient for phishing prevention.
- The 2-out-2 feature of visual cryptography provides effective collaboration of images at the Certified .

METHODOLIGIES

TO PREVENT PHISHING

- Microsoft Phishing Filter uses a combination of Microsoft’s URL Reputation Service (URS) and local heuristics built into the IE 7 browser.
- Netscape Browser 9.0 includes a built in phishing filter which relies solely on a blacklist, which is maintained by AOL and updated frequently.
- McAfee's Site Advisor product is a free stand-alone anti phishing product. Suspect or blocked sites are identified by a popup balloon and by color and text changes in the button.

STEGANOGRAPHY

- **Text-Based Steganography**: It makes use of features of English Language like inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a statement .
- **BPCS Steganography**: The information hiding capacity of a true color image is around 50% . A sharpening operation on the dummy image increases the embedding capacity quite a bit. Randomization of the secret data by a compression operation makes the embedded data more intangible. The steganography program for each user is easy. It further protects against eavesdropping on the embedded information. It is most secured technique and provides high security.

VISUAL CRYPTOGRAPHY

- **Halftone visual cryptography**: This novel technique achieves visual cryptography via half toning. Based on the blue-noise dithering principles, this method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information.
- **2-0ut-2 Visual Cryptography**: Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares .

ALGORITHMS

BPCS (Bit-Plane Complexity Segmentation) STEGANOGRAPHY ALGORITHM

The algorithm can be described in concise steps as follows .

- ❖ Convert the carrier image (of any file-format) from PBC (Pure Binary Code) to CGC (Canonical Grey Code) system and in png format.
- ❖ Perform the histogram analysis.
- ❖ After that bit-plane analysis is performed.
- ❖ Perform size-estimation i.e. calculate the places where we can store the secrete image.
- ❖ Perform bit plane complexity segmentation on image i.e. embed secrete blocks into carrier image.
- ❖ After embedding mail that image to another user.
- ❖ For extracting the embedded image performs de-steganography which is exactly opposite to steganography.

VISUAL CRYPTOGRAPHY ALGORITHM

- ❖ Visual cryptography is a type of cryptography which allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system.
- ❖ Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process.
- ❖ This is equivalent to using the logical OR operation between the shares .

LINKGUARD ALGORITHM

- LinkGuard works by analyzing the differences between the visual link and the actual link.
- It also calculates the similarities of a URI with a known trusted site.

ARCHITECTURE

EXISTING SYSTEM

The traditional method of online shopping involves customer or end-user selecting items online shopping portal and directing it to the payment gateway. Different payment gateways have different mechanism of storing detailed information of consumer. There have been recent high profile breaches such as in Epsilon, Sony’s PlayStation Network and Heartland Payment Systems show that card holders’ information is at risk both from outside and inside.

DRAWBACK

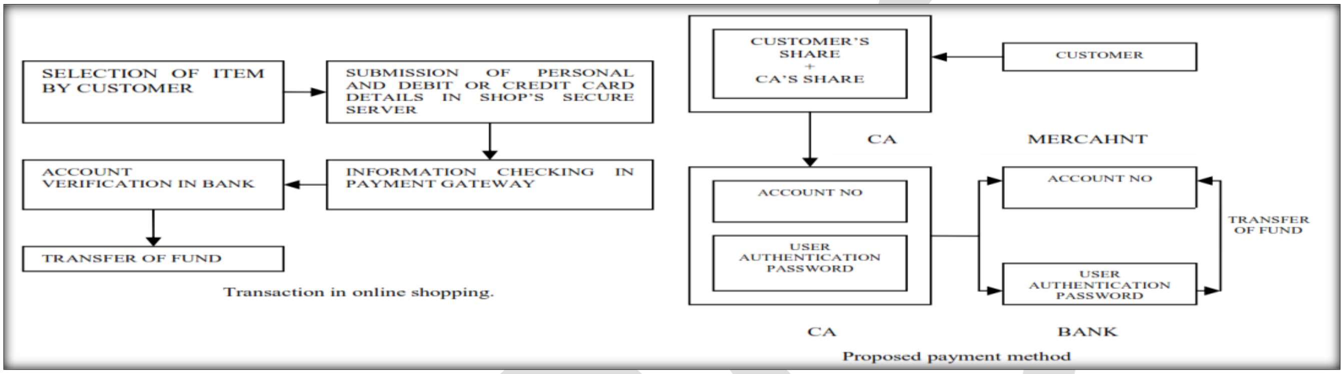
In the traditional system mentioned above, customer is not sure whether his PIN No and CVV No is sent to the merchant. One still has to trust the merchant and its employees to use card information for their own motives. This representation doesn’t show high level security. In these traditional systems, there is no additional non-functional requirement of phishing mechanism which can be harmful and might lead to employment of social engineering and technical subterfuge. Thus, in the proposed system mentioned later in this paper would ensure better security and satisfaction of consumer or other transaction stakeholders.

PROPOSED SYSTEM

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer.

In the proposed method, customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method as mentioned in section IV. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken. Fromthe snapshot image, two shares are generated using visual cryptography.

Now one share is kept by the customer and the other share is kept in the database of the certified authority. During shopping online, after selection of desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits its own share and merchant submits its own account details. Now the CA combines its own share with shopper's share and obtains the original image. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

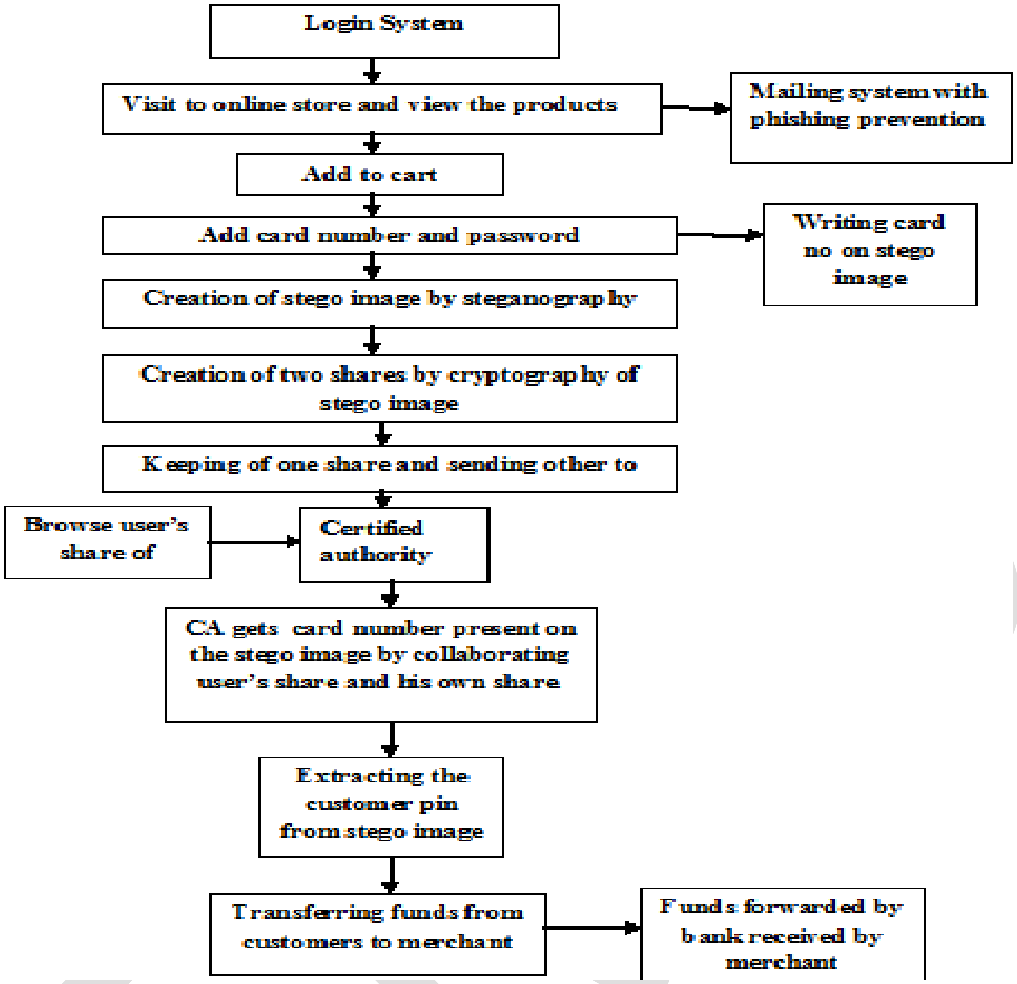

SELECTION OF ITEM BY CUSTOMER
SUBMISSION OF PERSONAL AND DEBIT OR CREDIT CARD DETAILS IN SHOP'S SECURE SERVER
ACCOUNT VERIFICATION IN BANK
INFORMATION CHECKING IN PAYMENT GATEWAY
TRANSFER OF FUND
CUSTOMER'S SHARE + CA'S SHARE
CUSTOMER
CA
MERCAHNT
ACCOUNT NO
USER AUTHENTICATION PASSWORD
ACCOUNT NO
USER AUTHENTICATION PASSWORD
TRANSFER OF FUND
CA
BANK

Transaction in online shopping.

Proposed payment method

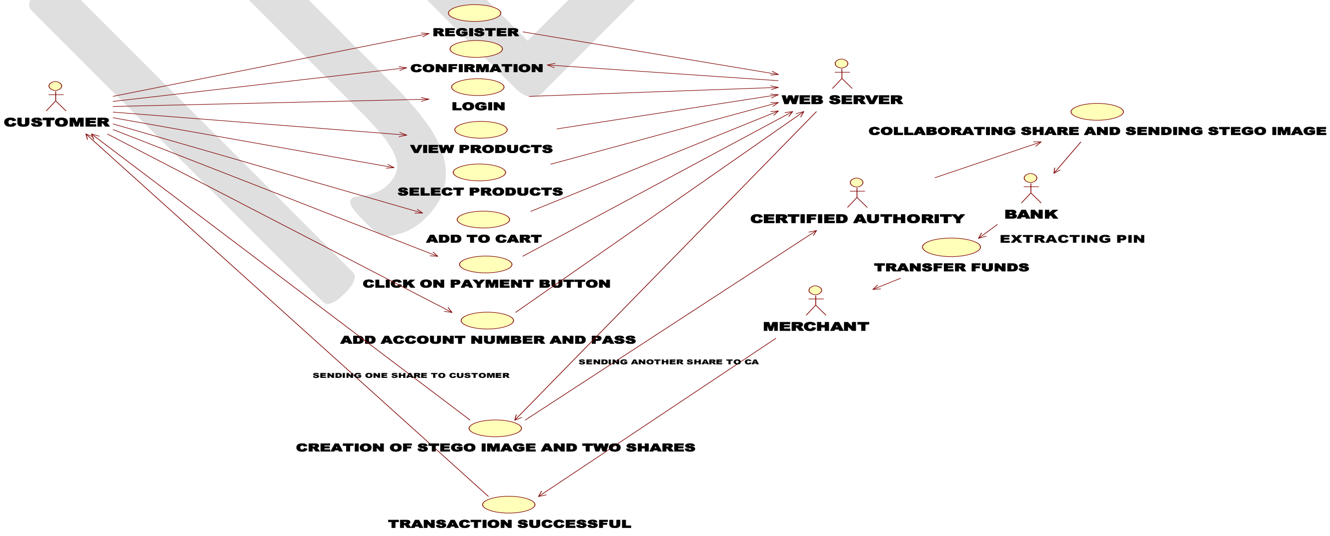
WORKFLOW DIAGRAM

In our system of online shopping, user logs in and enters into the online store to view the products. When he/she adds the item to the cart, he/she will be entering the card no and unique authentication password. This information will be created as a stego or stegno image using BPCS Steganography. 2-out-2 algorithm of visual cryptography will create two shares out of the stegno image. (Customer's share and CA's share). CA browses user's share and generates the card no which is sent to the bank so as to extract the customer's PIN (de-steganography). Finally fund will be transferred from the bank to the merchant.

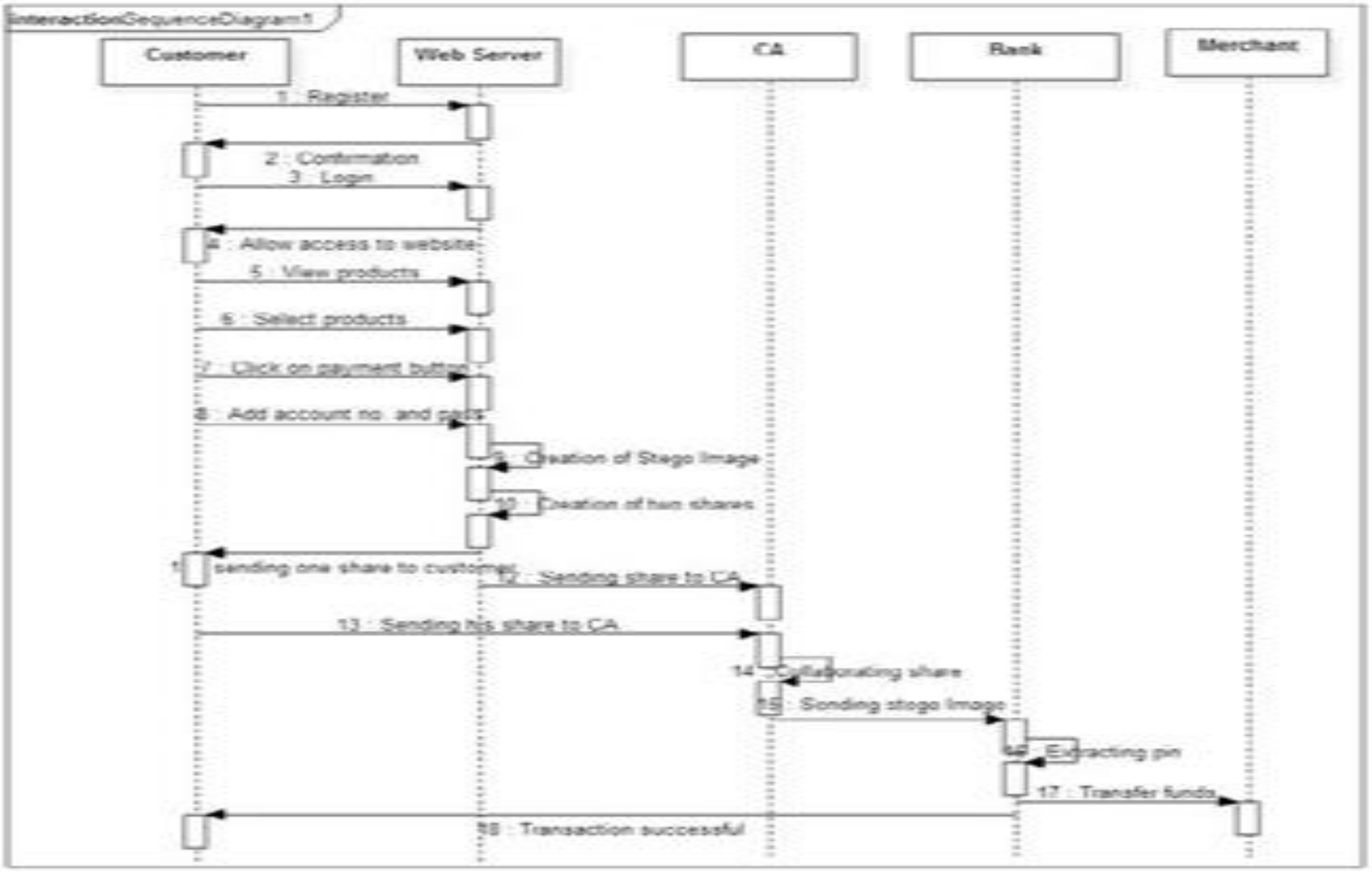

Login System
Visit to online store and view the products
Mailing system with phishing prevention
Add to cart
Add card number and password
Writing card no on stego image
Creation of stego image by steganography
Creation of two shares by cryptography of stego image
Keeping of one share and sending other to
Browse user's share of
Certified authority
CA gets card number present on the stego image by collaborating user's share and his own share
Extracting the customer pin from stego image
Transferring funds from customers to merchant
Funds forwarded by bank received by merchant

USE CASE DIAGRAM

The Use Case Diagram shows the interaction between the elements.



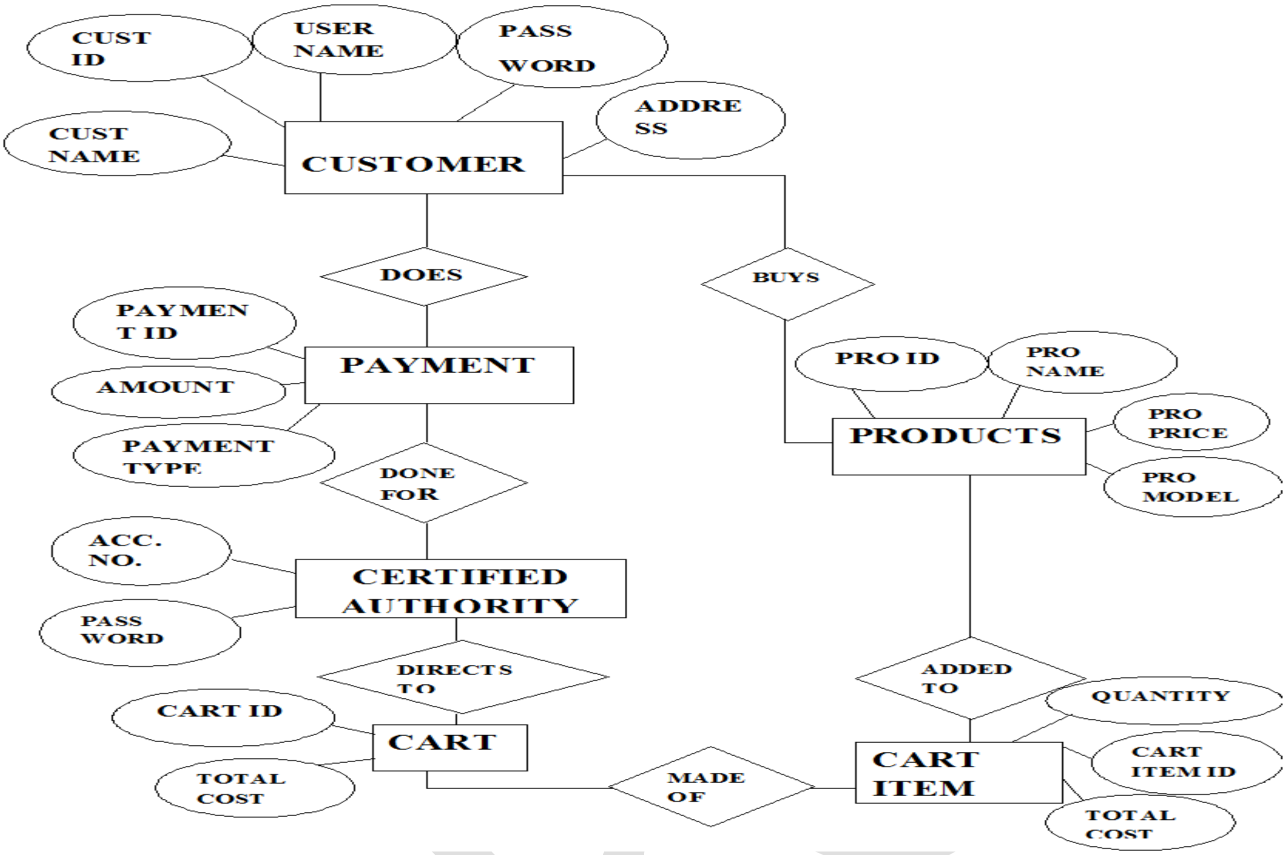
SEQUENCE DIAGRAM


interactionSequenceDiagram1
Customer
Web Server
CA
Bank
Merchant
1 : Register
2 : Confirmation
3 : Login
4 : Allow access to website
5 : View products
6 : Select products
7 : Click on payment button
8 : Add account no. and pass
9 : Creation of Stego Image
10 : Creation of two shares
11 : sending one share to customer
12 : Sending share to CA
13 : Sending his share to CA
14 : Collaborating share
15 : Sending stego Image
16 : Extracting pin
17 : Transfer funds
18 : Transaction successful

The Sequence is as follows: The user registers with the web server and gets the confirmation.Now the user logs in views and selects the available products. The user then clicks on Add To Cart button.After clicking on the payment button the web server takes a snapshot of customer unique authentication password and customer authentication information.Stego image and Two shares are created by using Visual Cryptography algorithm. One share is sent to customer and another share is sent to Certified Authority. The Certified Authority collaborates the share and sends the stego image to the bank. The bank extracts the pin and performs successful fund transfer between the customer and the merchant.

ENTITY RELATIONSHIP DIAGRAM

The ER Diagram depicts the graphical relationship between the entities and their relationships among them. The entities contains number of attributes. Customer, Products, Cart Item, Cart, Certified Authority and Payment acts as entities. Two entities are connected by using the relationship symbol. Customer acts as the entity and the attributes of Customer are CUST NAME, CUST ID, USER NAME, PASSWORD, ADDRESS. The Customer after filling the registration form buys products and adds to cart. The add to cart items will be directed to Certified Authority.



III. RESULTS AND DISCUSSIONS

TEXT BASED STEGANOGRAPHY METHOD

- Proposed text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence.
- Number assignment method is used to maximize no of letters in a particular assigned number group which in turn gives flexibility in word choosing and ultimately results in suitable sentence construction**.**

A. ENCODING:

- Representation of each letter in secret message by its equivalent ASCII code
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.

TABLE I. NUMBER ASSIGNMENT

Letter	***Number assigned***	***Letter***	***Number assigned***
E	**15**	**M**	**7**
A	**14**	**H**	**7**
R	**13**	**G**	**6**
I	**13**	**B**	**5**
O	**12**	**F**	**4**
T	**11**	**Y**	**4**
N	**11**	**W**	**3**
S	**10**	**K**	**3**
L	**10**	**V**	**3**
C	**9**	**X**	**2**
U	**8**	**Z**	**2**
D	**8**	**J**	**1**
P	**7**	**Q**	**0**

- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Encoding is not case sensitive.

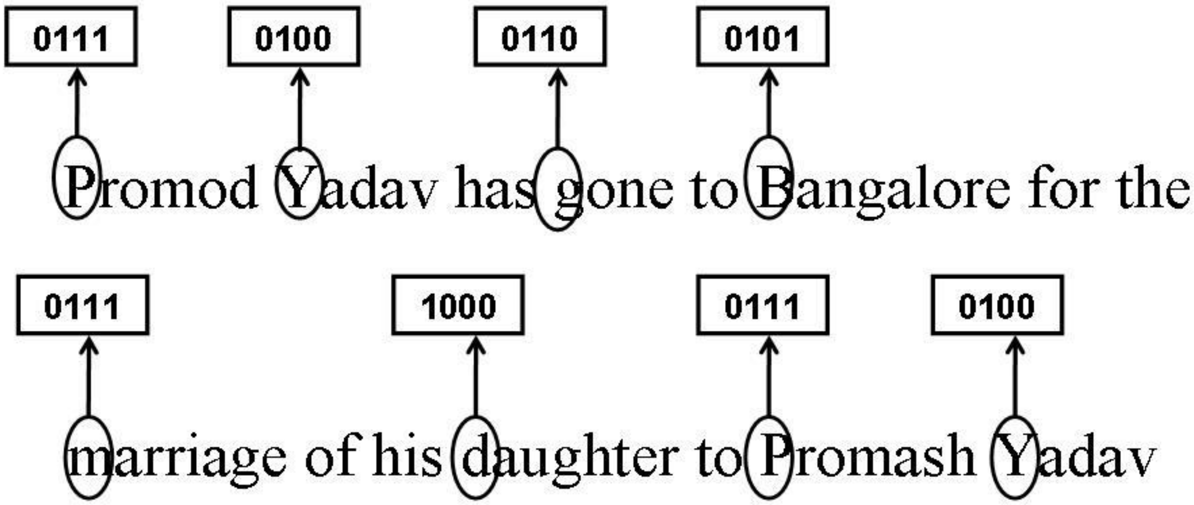
B. DECODING

- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

C. RESULT

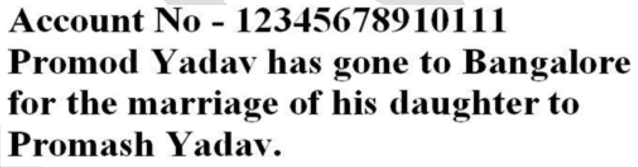
To implement the above text based steganography method, a secret message is considered as "text".

Text = 01110100011001010111100001110100


0111
0100
0110
0101
Promod Yadav has gone to Bangalore for the
0111
1000
0111
0100
marriage of his daughter to Promash Yadav

VISUAL CRYPTOGRAPHY ALGORITHM

- Visual cryptography is a type of cryptography which allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system.
- Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image.



Account No - 12345678910111
Promod Yadav has gone to Bangalore
for the marriage of his daughter to
Promash Yadav.

FIGURE 3.2.1 SNAPSHOT ACCOUNT NO AND COVER TEXT

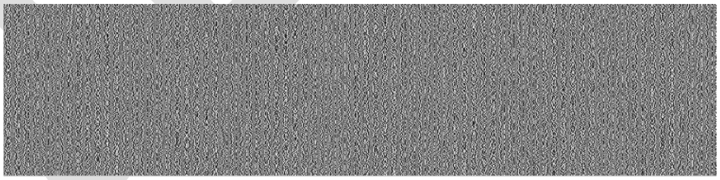


FIGURE 3.2.2SHARE 1 KEPT BY CUSTOMER

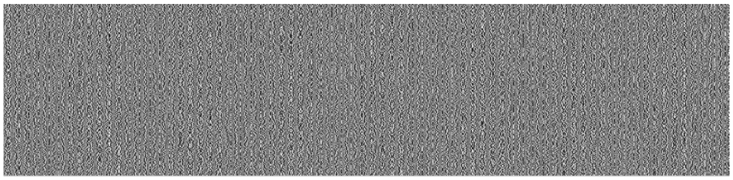
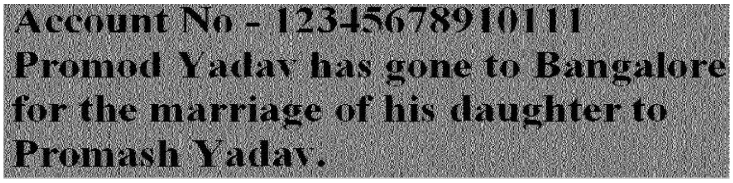


FIGURE 3.2.3 SHARE 2 KEPT BY CA



Account No - 12345678910111
Promod Yadav has gone to Bangalore
for the marriage of his daughter to
Promash Yadav.

FIGURE 3.2.4 OVERLAPPING OF SHARE 1 AND SHARE 2

IV. CONCLUSION

In our project, a payment system for online shopping is proposed by combining BPCS steganography and 2-out-2 visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. BPCS Steganography is really effective against eavesdropping and has a high information hiding capacity as compared to traditional steganography approach. The method is concerned only with prevention of identity theft and customer data security. The main aim is consumer satisfaction and authorized merchant-bank interaction for fund transaction. In comparison to other banking application which uses steganography and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

REFERENCES:

[1] Souvik Roy, P.Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science,2014.

[2] Pranita P. Khairnar, Prof. V. S. Ubale, " Steganography Using BPCS technology,"in Proc. International Journal Of Engineering And Science , May 2013. Vol.3(Issue 2),pp 08-16.

[3] U.Naresh, U.VidyaSagar, C.V. MadhusudanReddy , " Intelligent Phishing Website Detection and Prevention System by Using Lin Guard Algorithm," in Proc. IOSR, 2013. Vol. 14(Issue 3), pp 28-36.

[4] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.

[5] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.

[6] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.

[7] ChetanaHegde, Manu S, P DeepaShenoy, Venugopal K R, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,",in Proc. 16th IEEE International Conference on Advanced Computing and Communications,2008.

[8] Juan Chen, ChuanxiongGuo, "Online Detection and Prevention of Phishing Attacks," Proceedings of First International Conference on
Communications and Networking in China (ChinaCom '06), pp. 1 - 7,Beijing, China, 2006.

[9] J. Chen, T. S. Chen, M. W. Cheng, “A New Data Hiding Scheme in Binary Image,” Proceeding of Fifth International Symposium onMultimedia Software Engineering, pp. 88-93, 2003.

[10] Daniel Gruhl, Anthony Lu, Walter Bender, “Echo Hiding,” Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.

[11] https://www.braintreepayments.com/blog/pci-compliance-and-the-cost-of-a-credit-card-breach.

[12] http://oxforddictionaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english