ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Securing Transactions in E-Commerce using Visual Cryptography and Steganography

T. Venkat Narayana Rao
Professor, Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Karnati Yashwanth Reddy
Student, Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Ganji Dinesh Kumar
Student, Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Abstract: The Contemporary world has seen a tremendous usage of E-Commerce because of its appliance. The Information confidentiality is one of the major requirements to the users of Online Banking Systems. The issue with traditional Online banking applications is that they need to send the sensitive contents associated with the transaction such as Personal Identification Number (PIN), One Time Password (OTP) to the targeting customers in the form of plaintext, which is vulnerable to unauthorized access. Personal Identity theft and phishing attack are common threats of online shopping. Phishing is a technique which involves unauthorized gaining of sensitive information like password, bank details, credit card details from victims, often for malicious reasons, by pretending as a trustworthy entity in an electronic communication. It is a social engineering technique used to mislead users. The solution to the above consequences requires a software application that holds proficient encryption procedures. To enhance the security of the content on the internet, this paper proposes a technique that introduces an idea of Visual Cryptography and Steganography. These methods represent a new approach which would provide a confined information for the fund transfer. The method ensures the security to the customer's data and decreases customer's risk thus preventing identity theft.

Keywords: Online shopping; identity theft; Phishing; Visual Cryptography; Steganography

I. INTRODUCTION

Increase in quantum of E-Commerce transactions has changed the way business has been conducted all over the world. In this age of universal digital connectivity, of viruses and hackers, Debit or Credit card fraud and data confidentiality are major concerns for customers, merchants and banks. Online Shopping includes retrieval of product information from the Internet and generation of purchase order through electronic purchase request, filling of payment details such as credit or debit card information and finally shipping of product by mail order or home delivery by courier [1]. Identity theft, skimming and phishing are the common threats of online shopping. Identity theft is intentional use of someone else's information, often for malicious reasons such as to gain a financial advantage or other benefits in the other person's name. It may happen when there is a loss of confidentiality. In 2012 consumer information was misused for an average of 48 days as a result of identity theft [2]. Phishing is a security breach which uses sophisticated techniques for luring the victims in order to gain user's financial information and password data. Payment Service, Financial and Retail Service are the most concentrated industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption safeguards the consumer information in transit between the consumer and the online merchant. However, one must still depend on merchant and its employees to accomplish their task [3].

The main intent of this paper is to provide high level security in E-Commerce applications and online shopping. The transaction performed using the proposed algorithms helps in minimizing detailed information communicated between consumer and online merchant and enables successful fund transfer thereby preserving consumer information and preventing abuse of information at merchant's side. This is achieved by the introduction of Central Certified Authority (CA) and combined application of text based Steganography, Visual Cryptography and Digital Signature for this purpose. Steganography is the art of hiding of a secret data inside another data so that hidden message is indistinguishable. Visual Cryptography (VC), is a cryptographic technique based on sharing of visual secrets used with image encryption.

II. EXISTING SYSTEM

The three main entities involved in the existing system are customer or client, merchant server and bank server. The customer first creates an account with the merchant server by filling username, password, e-mail address, credit card information and other confidential information in order to login merchant site. If login is successful, the customer will choose a product which he intends to purchase and makes purchase request. After that, the merchant forwards the customer's payment information to the payment portal to process the payment. In turn the bank server send One Time Password (OTP) to client in order to authenticate the request made by the client. At client side, the OTP is validated and purchase order is made by the client. The three entities and their functions are shown in Fig.1.

A. Problem Statement

The traditional system mentioned above, is vulnerable to different types of attacks. The merchant server, through which the customer payment information is delivered to the payment portal may be compromised. The customer is also not sure whether his PIN No and Card Verification Value (CVV) No is sent to the merchant or not. However, one still has to trust the merchant and his employees to use the card information for

the transactions. This system doesn't represent high level security. In these traditional systems, there is no additional nonfunctional requirement of phishing mechanism which can be risky and might lead to employment of social engineering and technical subterfuge. Thus, in the proposed system mentioned in this paper would guarantee better security and satisfaction to consumer or other transaction stakeholders.

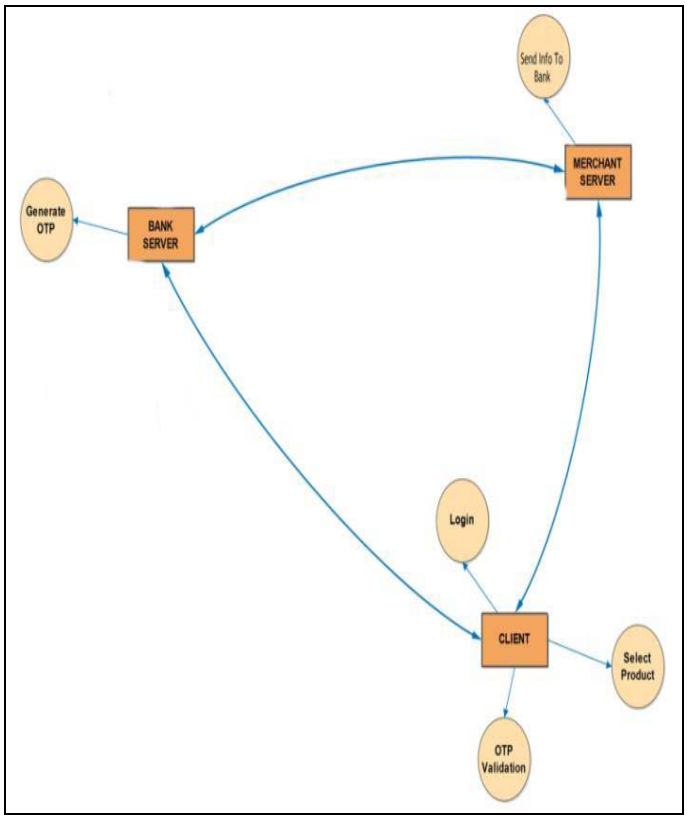


Figure 1. Current Mechanism

III. PROPOSED SYSTEM

In the proposed system, information given by the customer to the online merchant is confined to limited information that will only authenticate the payment made by the said customer with the help of proposed methodologies. This is implemented by the introduction of a trusted fourth party called central Certified Authority (CA) and combine the application of steganography and visual cryptography.

A. System Architecture

The information received by the merchant can be in the form of account number related to the card used for the shopping. The minimum information obtained by the merchant will only validate receipt of payment from authentic customer. Fig. 2 depicts the system process and is explained in the following steps:

- In the proposed method, customer unique authentication password in connection with the bank is hidden inside a cover text using the text based steganography.
- Customer authentication information (account no) with regard to the merchant is placed above the cover text in the form of plain text.
- Now a snapshot of two texts is taken.

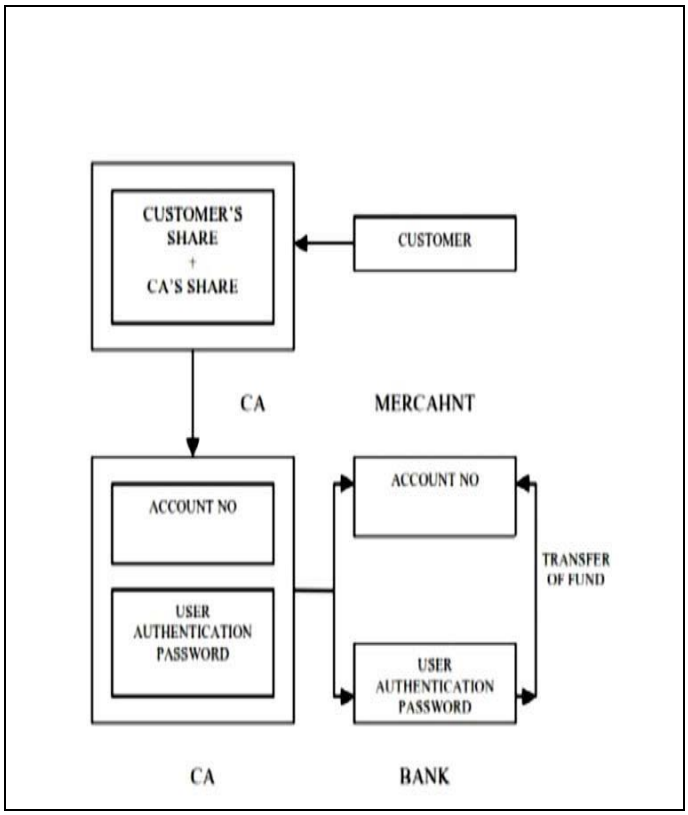


Figure 2. System Architecture Diagram

- Two shares are generated from a snapshot image 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 the process of online shopping, after selection of desired item from the catalogue 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 recovers the original snapshot image.
- Now the bank receives merchant account details, cover text from CA, where customer authentication password is recovered from the cover text using decoding algorithm of text-based steganography.
- Customer authentication information is sent to the merchant by CA.
- Upon recovering customer authentication password, bank verifies it for a match with its own database and after verifying genuine customer, transfers fund from the customer account to the submitted merchant account.
- After the amount is credited to the merchant's account, its payment system validates receipt of payment using customer authentication information.

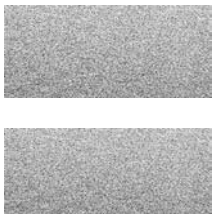
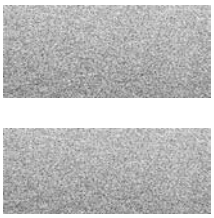
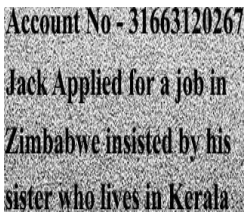
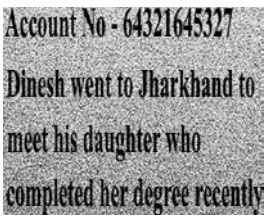
The problematic aspect is that CA does not know to which bank to forward the cover text obtained from combining two shares. It can be resolved by appending 9 digit routing or transit number of bank with customer authentication information.

The proposed technique is applied for transactions made by two different account holders. If customer unique authentication password is hidden in "text" and account no of customer is as shown in the table I, then the snapshot of cover text and account no, resultant shares generated by the application of visual cryptography on snapshot and the recovered image formed by overlapping of those two shares is shown in column 2 and column 3 of table II.

Table I. Account holder details

Sr. No.	***Name***	***Account number***	***Password/PIN***
1	K.Yashwanth	31663120267	5642
2	G. Dinesh	64321645327	3692

Table II. Formation of cover text and Generation of shares

	Account 1	**Account 2**
Snapshot account no and cover text	Account No - 31663120267 Jack Applied for a job in Zimbabwe insisted by his sister who lives in Kerala	Account No - 64321645327 Dinesh went to Jharkhand to meet his daughter who completed her degree recently
Generation of shares		
Overlapping of share 1 and share 2		

B. *Advantages*

- Proposed method minimizes the information shared between customer and online merchant. Customer is not affected even in the case of any compromise in merchant's database.
- Presence of a fourth party, CA that is trusted by the user community and it enhances customer's satisfaction and security further as more number of parties are involved in the process.
- Usage of steganography ensures that the customer authentication password is unrevealed to CA thus maintaining customer privacy.
- Sending Cover text in the form of email from CA to bank will not raise suspicion.

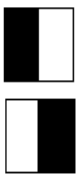
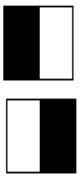
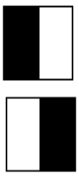
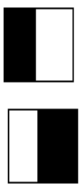
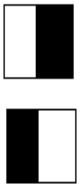
IV. METHODOLOGIES/ALGORITHM DETAILS

A. *Visual Cryptography*

Visual cryptography is a cryptographic technique used to encrypt image based data such as snapshot of any text, signature, pictures and diagrams etc. and decryption can achieve directly by human visual system, without the computation of computers [7]. In VC Scheme, the secret data splits into two or many shares, thereby making it impossible to know any information about the secret data without having both of them. The secret data can be recovered only when the desired numbers of shares are superimposed with one another. During decryption the generated shares are needed to be printed out in a transparency sheets/papers and needs overlap of all or desired number of transparencies with each other that reveals the secret information. Therefore, it does not require any complex calculation like other traditional cryptography schemes.

The basic idea of VC scheme is to generate shares for binary image which was initially proposed by Naor and Shamir [9]. Two-out-of-two VC scheme generates two shares such as Share 1 and Share 2. A single pixel is divided into two sub-pixels which is shown in Table III. If pixel is white then a coin toss is used to randomly choose one row among the top two rows to generate share1 and share2. If the pixel is black then a coin toss is used to randomly choose one row among the bottom rows to generate Share 1 and Share 2. A new coin toss is required in the encryption of each pixel to choose any of the following combination of shares. The pixel obtained as a result of superimposing each pixel of Share 1 and Share 2 is as shown in the last column of Table III.

Table III. Construction of a two-out-of-two VC scheme

Pixel		S1	S2	S1 + S2
	p = 0.5 p = 0.5			
	p = 0.5 p = 0.5			

If pixel is black then we would obtain two black sub pixels when two shares are superimposed. If pixel is white then we get one black subpixel and one white sub pixel respectively from the two shares. Hence, the reconstructed image has a grey level of 1 if the pixel is black and a grey level of 1/2 if the pixel is white. A 50% loss of contrast is observed in the recovered image, but it is still visible. The scheme is based on two Boolean matrices S_0 and S_1, also called basis matrices. In general k out of k shares and 2^{k-1} represents number of sub-pixels in each share. S_0 handles the white pixels, all 2^{k-1} columns has an even number of 1's and S_0 for 2×2 matrix is given in (1). S_1 deals with the black pixels, all 2^{k-1} columns has scheme, matrix size is $k \times 2^{k-1}$ where k represents number of an odd number of 1's and S_1 for 2x2 matrix is given in (2). There are two sets, the white set C_0 and black set C_1. These sets are defined as the collections of all matrices obtained by all possible permutations of columns in S_0 and S_1 and are given in (3) and (4) for a 2×2 matrix respectively. Each row of the S_0 and S_1 matrices represents a separate share [11]. The recovery of the secret image is performed through the OR operation (+) on the corresponding rows of any one of the matrix in the collection set [10].

$$S_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad (1)$$

$$S_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2)$$

C_0={all the matrices obtained by each of arrangements of columns in (1)}

C_1={ all the matrices obtained by each of arrangements of columns in (2)}

As such therefore;

$$C_0 = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \right\} \quad (3)$$

$$C_1 = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \quad (4)$$

Pictorial representations of visual cryptography scheme are shown in figure 3. Suppose any secret image say the dollar symbol to be sent secretly to authenticate recipient, then the VC scheme splits it into two shares such as share1 and share2. The information regarding the secret data would not revealed by any of these two shares individually. The secret data can be revealed only by stacking of these two shares i.e., the dollar symbol in this example.

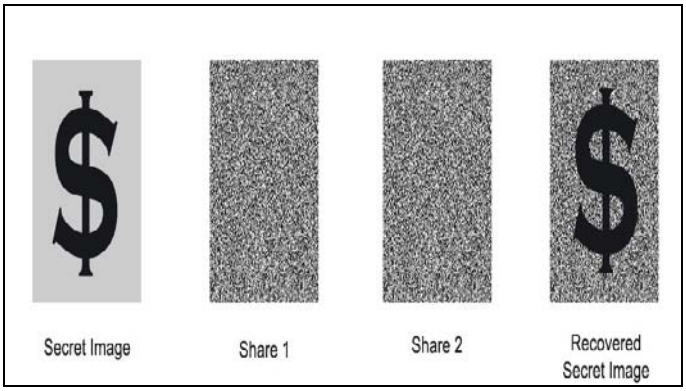


Figure 3. Visual Cryptography scheme for binary image

B. Extended Visual Cryptography for color images

The proposed algorithm is for encrypting color image, that presents a system which takes four pictures as an input i.e., one original image and three cover images. It generates three images which correspond to three of the four input pictures. These three images are generated using the three cover images. The decoding is achieved by selecting some subset of these 3 images. Thereafter, making transparencies of them, and stacking them on top of each other. Hence, the forth picture is reconstructed by printing the three output images onto transparencies and stacking them together as in [8]. The reconstructed image has the size equivalent to that of original secret image. The entire process is summarized in Fig. 4.

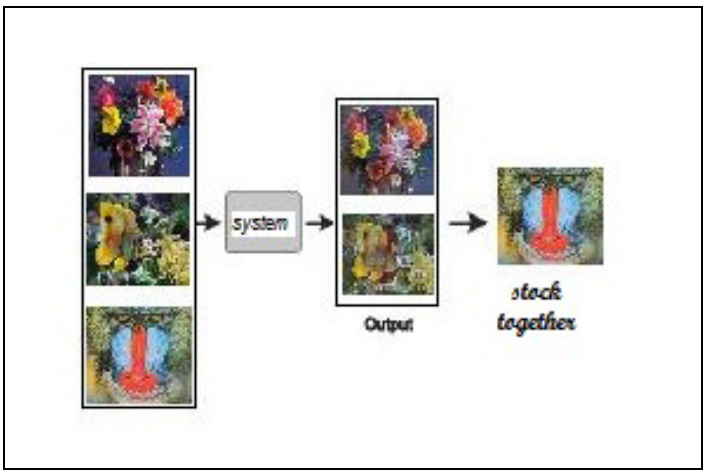


Figure 4. Visual cryptography system for color image

Every single pixel in the secret image is divided into subpixels in each share, which can be still perceived as a single pixel by Human vision system. The security of each share highly depends on the color composition of the original secret image. For recovering a secret image, the minimum requirement is that the cover image should at least be able to determine the shape or pattern of the original secret image, which is able to determine the boundary between two distinct

color regions in the image. In this paper, we are assuming an input 24-bit bitmap color image which each 3-byte sequence in the bitmap array represents the relative intensities of red, green and blue respectively for image sized 256×256 RGB pixel for hiding secret image. The following steps of the proposed algorithm illustrated by an example where the original secret image is a 24-bit color baboon image shown in Fig. 5.

Figure 5. Original secret image

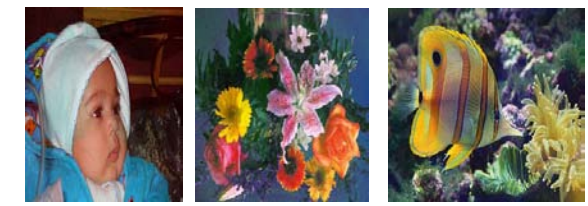
- The three primitive color images namely C (Cyan), M (Magenta) and Y (Yellow) are produced by the decomposition of secret image under subtractive model. The three primitive color components of the baboon image are shown in Fig. 6, where each image can hold 256 levels of the corresponding primitive colors, and each pixel is defined by three bytes. Converting to (C,M, Y) where C,M,Y Є {0- 255}.

Figure 6. Primitive Color (C, M, Y) Components

- For each pixel of the primitive component $P_{i,j}$ to be able to store it in the other image, reduce the $P_{i,j}$ value by holding ¼ $P_{i,j}$. The color of a pixel in the original baboon secret image in terms of primitive cyan, magenta and yellow with reducing value, respectively is shown in Fig. 7.

Figure 7. Reducing pixels value of (C,M,Y)

- The number of cover images required is equal to the number of primitive color components. There are three primitive color components, therefore we need three cover images in order to generate three shares.



(a) (b) (c)

Figure 8. The Generation of C, M, Y Shares

- In this step, three shares, namely a, b and c are generated as shown in Fig. 8, where each share contains a part of secret image. These shares are generated by reading pixel by pixel from the reduction primitive-color images of the original secret image C,M,Y and mixing(OR operation) together with ¾ pixel of cover image. For example if the pixel value of primitive color equal 00000011 and the value of the cover image is 01101100 the output pixel will be 01101111 by OR operation. So, each share (a, b, and c) hold part a primitive color for secret image, From the figure, a baby image in share (a) holds C primitive color, flower image in share (b) holds M primitive part, and fish image in share (c) holds Y primitive color, selecting of the cover image depending on minimum differences between pixel in cover image and primitive color in secret image.
- Repeat step 1 to 4 for each and every pixel of the original image. To recover the secret original baboon image it is necessary to removing the unwanted color in each share by the operation 255 minus ¾ $CP_{i,j}$, where $CP_{i,j}$ is the pixel of the cover image in the share (a,b,c).

C. Proposed Text-based Steganography method

Steganography is an art of hiding information inside another data [12]. The main objective of steganography is to safeguard the contents of secret information. This technique, communicates secret information through cover data which is unknown carrier. Carrier's data could be many forms such as images, audio, video, text or any other data. In steganography, the image media are most popular as a carrier/cover data because of the presence of large number of redundant bits in it. The hidden information may be normal text or cipher text. The encoding and decoding process of basic steganography technique is shown in Fig. 9.

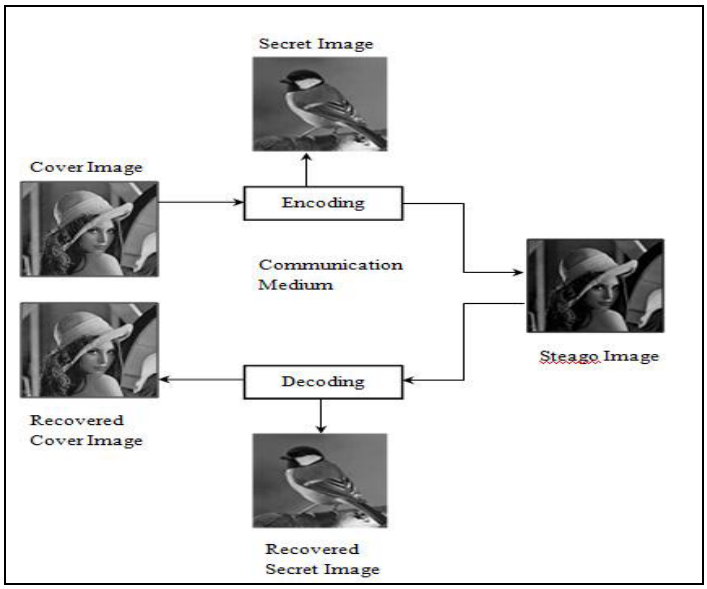


Figure 9. Encryption and decryption process of Steganography technique

The proposed text based steganography technique uses the characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding of secret data as in [4] [5] [6]. Each letter is assigned a number in the range of 0 to 15 as shown in the table IV. For different frequencies, different numbers are assigned to the letters. Number are assigned in the range (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is any integer from 0 to 11. This method is used to maximize number of letters in a particular assigned number group which would provide flexibility in word choosing and ultimately results in appropriate sentence construction[12].

1) ***Encoding Steps:***

- Represent each letter in secret message by its equivalent ASCII code. e.g. A-65.
- Conversion of ASCII code to equivalent 8 bit binary number. e.g. 65 – 01000001.
- Division of 8 bit binary number into two parts each of 4-bits. e.g. 01000001 – 0100 and 0001.
- Choosing of suitable letters from table IV corresponding to the 4 bit parts. e.g. 0100 – y and 0001 – j.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words
  e.g. y – Yadav
- Converted sentence can be generated as secret key image.
- Encoding is not case sensitive.

2) ***Decoding Steps:***

- First letter in each word of cover message is taken and corresponding 4 bit number is identified from table IV.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are recovered from 8 bit numbers.
- The letters of the secret message from the corresponding ASCII codes are identified.
- Finally secret message is recovered from ASCII codes.

3) ***Result:***

To implement the above text based steganography method, let us consider the secret message “5642”. The ASCII equivalents for each digit are 53,54,52,50 respectively. The 8-bit binary code for each ASCII number is generated and the following “text” is formed. The text is 00110101001101100011010000110010. Result of encoding is shown in Fig. 10.

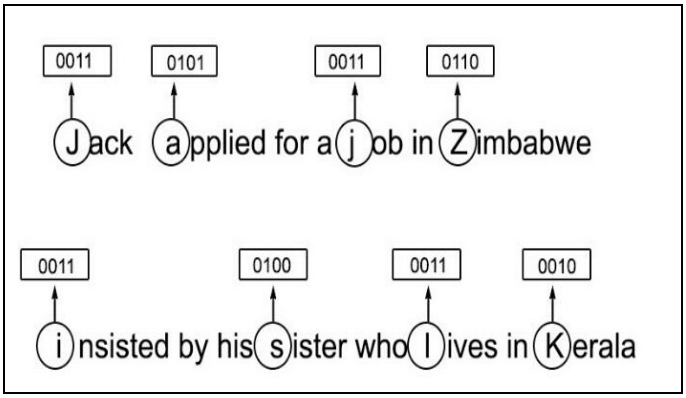


Figure 10. Cover message

Table IV. NUMBER ASSIGNMENT

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

D) ***Hybrid Approach***

Steganography followed by Visual Cryptography:

The data security is improved when the cryptography technique is integrated with the other security mechanism such as steganography. Hybridization can be achieved in various ways [13].

- First encrypt the secret data using VC scheme and then embed that encrypted data using steganography technique.
- First embed the secret data inside any cover data using steganography technique and then visual cryptography techniques can applied on it.

The proposed system follows second approach of hybridization. In this approach, first secret image is hidden inside a cover image using text-based steganography and then the embedded image (stego image) is divided into different shares using visual cryptography scheme. It provides more security to the secret data.

V. RESULTS AND DISCUSSION

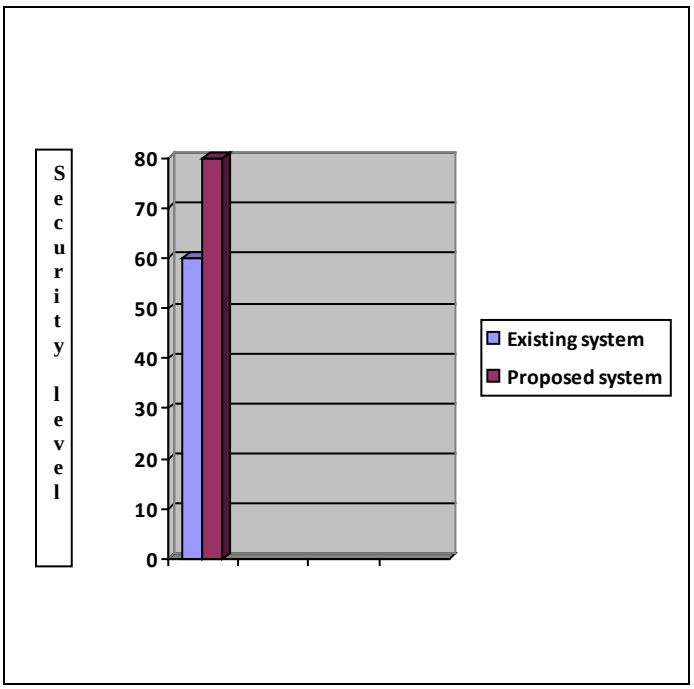


Figure 11. Resultant Proposed Output

The graph shown in Fig. 11 depicts us that there is an increase in the level of security in the proposed system compared to existing system. System performance is tested under different conditions and system security is observed to be much higher. We require less login time to invoke this system.

In the proposed color VC scheme, the number of pixels in the decoded image is same as in the original secret image because the pixel p is not expanded. The size of secrete image must be smaller or equal to the cover images as there is a need to store ¼ pixel of secret image with the ¾ pixel of cover image in order to produce a share. After testing many different images from different colors and in resolution it was observed that the proposed algorithm could not take dark image significantly with high contrast and which subsequently generate the unclear share, and they appear as corrupted images with large amount of noise data making it easier to detect.

The processing which is added to change the quality of color of a recovered secret image is done after removing unwanted color from the share i.e. subtraction of ¾ $CP_{i,j}$ and before stacking the shares together. In this context the processing refers to changing pixel value from ¼ $P_{i,j}$ to $P_{i,j}$ by multiplying with 4 to get full value from 255.

The way of reduction in original pixel and subtractions of the original pixel with previous shares pixel offers more sensitive results and with better color quality. The results suggest that the security of the image depends critically on the color composition and distribution of the original secret image.

In the proposed text-steganography technique, to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility and meaning in sentence construction. So to conceal a large message, this technique necessitates large number of words and makes sentence construction complex. Therefore, it also creates complexity in the process of decoding of a secret message. The disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information.

VI. CONCLUSION

The proposed integration of text based steganography and visual cryptography provides confidentiality of customer data and prevents fraud at merchant's side. The main focus of this paper is to address issues relating to the identity theft and customer data security along with the phishing problem. The system ensures the authentication of both client as well as merchant server. Shares may contain customer image or signature in addition to customer authentication password. In VC scheme, the future work focuses on improving the contrast and producing more clear resultant secret image. Further extension of this work is needed to use this technique with other format of color images. Increase in number of shares in visual cryptography helps us to compare the improvement in quality. The proposed payment system can also be extended to physical banking.

VII. REFERENCES

[1] 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.

[2] Javelin Strategy & Research, "2013 Identify Fraud Report," https://www.javelinstrategy.com/brochure/276.

[3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report, 2013," http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf .

[4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.

[5] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[6] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004 – 2013.

[7] Rohith S and Vinay G – "A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme," International Journal Of Computational Engineering Research / ISSN: 2250–3005, Vol. 2, Issue No.3, pp-642-646, May-June 2012.

[8] Sozan Abdulla, "New Visual Cryptography Algorithm for Colored Image," journal of computing, Vol 2, Issue 4, April 2010, ISSN 2151-9617.

[9] M. Naor, A. Shamir, "Visual Cryptography," In Proceeding of Advance in Cryptology- EUROCRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, 950, pp. 1-12, 1995.

[10] Abdullah Jaafar, Azman Samsudin, "A Survey of Black-and-White Visual Cryptography Models," International Journal of Digital Content Technology and its Applications , August 2012.

[11] Z. Tifedjadjine, "Halftone Image Watermarking Based on Visual Cryptography," M.Sc. thesis,Batna University, Algeria, 2005.

[12] V. Lokeswara Reddy, A. Subramanyam, P. Chenna Reddy "Implementation of LSB Steganography and its Evaluation for Various File Formats," Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011).

[13] Moumita Pramanik1, Kalpana Sharma2, "Analysis of Visual Cryptography, Steganography Schemes and Analysis of Visual and its Hybrid Approach for Security of Images," International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014).