Secure Online Payment Approch using Postern Algorithm

Garima Gupta
Department of Computer Science Engineering
(Sager Institute of Research and Technology – Excellence, Bhopal, RGPV, India)

Sumit Dhariwal
Department of Computer Science Engineering
(Sager Institute of Research and Technology – Excellence, Bhopal, RGPV, India)

ABSTRACT
Secure online payment is one of the important issues in today's world. Online payment system as part of our daily routine life activities, gives many operation that remotely reduces human effort and make life easy in banking, online shopping, bill payments and ticket booking etc. In this proposed method present a secure online payment system which is based on two level security approaches. This proposed method presents a secure online payment system which is based on two level security approaches. In the first level Account number and OTPs are inserted in a image and the image is reshuffled and embedded into a cover image and then sent to receiver end. In encryption, information is transformed in such a way that it cannot be detected by hacker. Performance parameter result like PSNR and MSE in proposed method show good result in terms of visually. Some method shows good PSNR and other parameters but visually do not show good pixel values. Proposed Scheme shows good result in terms of visually as well as standard parameters.

Keywords
Online banking, PSNR, MSE, one time passwords (OTP)

1. INTRODUCTION
The last decade has witnessed a remarkable growth of internet users in India and all over the world. There are one hundred and thirty seven million internet users in India with 11.4 per cent penetration (Internetworldstats.com). It is predicted that number of internet users in India will reach to at least 350 million users by 2016 up from now predicted. Such growth is primarily attributed to investment by telecom carriers in high-speed wireless infrastructure and slashing prices of smart phones (online.wsj.com). The promising growth of internet users in India as well as world-wide (566.4 %, 2000-2012) (internetworldstats.com) has presented an optimistic view of future of internet banking in India. Hence, banks are investing huge amount in the infrastructure to host internet banking activities. In the era of digitalization online payment systems are increases day to day not only is terms online banking as well as in terms of other payments system like on money valets, Pay TM, debit cards and others.

The main concern of this paper to focus on secure online payment system.The present status of e-banking services in worldwide with respect to ATMs, Internet Banking, Mobile Banking, Credit Cards and Non-cash retail payments and use in daily life. The security & privacy issues and regulatory environment of e-banking services in these areas. For secure online payment system require to examine and compare the

Pre-login and Post-login security and privacy features of selected banks online banking portals. Also need to measure and compare the level of security and privacy concern among customers of selected banks regarding the use of e-banking services and compare the level of security and privacy satisfaction among customers of selected banks regarding use of e-banking services.

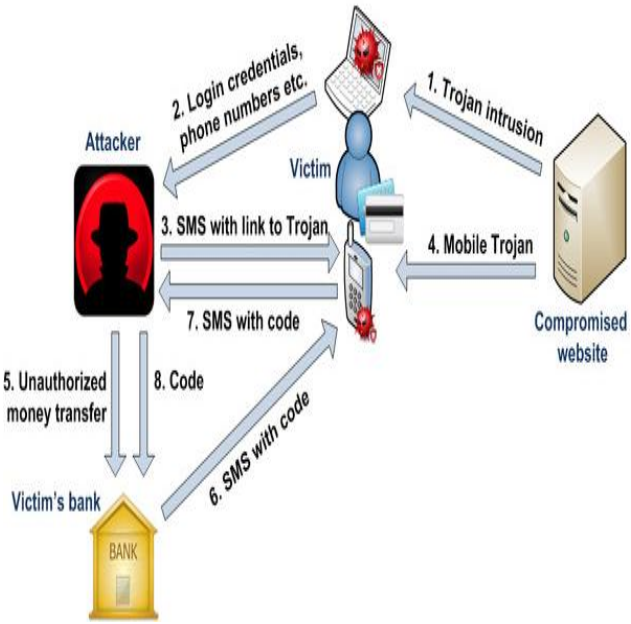


Figure1: Loop Holes in Online Bank System

2. ATTACKS IN ONLINE BANKING
There are different security issues in secure online banking. Different type of attacks in online banking. Security is the main issue for both online banking and E banking. There are different type of attacks occur in the Net banking and E-banking

Phishing: Phishing is a kind of scam where the scammers masquerade as a trustworthy source in attempt to gain private data such as PINs, and credit card details etc. through the internet

Malware: Malware, mainly spyware, is malicious software camouflaged as legitimate software planned to accumulate and transmit private data, such as PINs, without the customer's consent or knowledge.Identity theft: Identity theft is a crime in which a fraudster obtains key pieces of personal data, such as bank information, date of birth or driver's license numbers, in order to impersonate somebody.

Trojan horse/Trojan: Trojan horse are the most dangerous type of attack in which attacker can directly gain unauthorized access to victims systems

Virus: Virus is a computer program that designed to replicate itself from one computer to another.There are major attacks occurs in online banking and E-banking.

3. SECURE SOLUTION

There are different data hiding methods and techniques are available, these techniques are used secure online banking and E banking for secret data and secret communication in public channel like steganography, cryptography and others.

Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, data integrity, and of data authentication. In cryptography a plain message is encrypted into cipher text and that might look like a meaningless jumble of character whereas in case of steganography, the plain message is hidden inside a medium that looks quite normal and does not provide any reason for suspecting the existence of a hidden message. Such an image is called as stego-image. Data hiding conceals the existence of secret information while cryptography protects the content of messages. More and more attention is paid to reversible data hiding in encrypted images.

Steganography is the process in which hide the secret data in the cover image with secure key. Cover-Image: Original image which is used as a carrier for hidden information. Message: Actual information which is used to hide into images. Message could be a plain text or some other image.Stego-Image: After embedding message into cover image is known as stego-image.Stego-Key: A key is used for embedding or extracting the messages from cover-images and stego-images.

Postern Approach

Postern approach is the combination of image steganography and image cryptography.

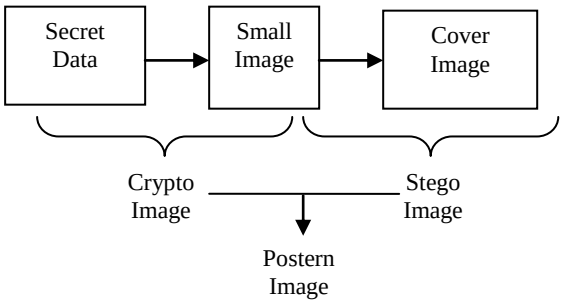


Figure 2: Shows the Postern Image Process Block

4. PROPOSED METHOD

The structure of proposed method is broadly divided into the two parts. Transmitter end and receiver end. The transmitter end is described first. The transmitter end is based on encoder part .This end generates the information and also creates the crypto image (CI) and postern image (PI).

Transmitter end (Encoder Part)

The transmitter end is the important part of the proposed method. The transmitter end is also known as an encoder part of the proposed method. In this part we create the crypto image. Crypto image is the summation of secret data . This crypto image hides into a cover image (CI) to generate postern image (PI). In this part there are four important terms used here.

- Secret Data (SD)
- 2.Crypto Image (CTI)
- 3.Cover image (CI)
- 4.Postern image (PI)

Secret Data (SD)

Secret data is the data which we want to hide. The quality of proposed work is based on the secret data. Secret data is generated at the user end and embedded into the small image. Similarly that secret data is obtained at the receiver end by postern image (PI). There is different type of secret data probable based on user end. In general secret data is in binary form, images and also ASCII based data available.

Crypto Image (CTI)

For embedding of secret data first apply cryptography and add secret data into 64X64 small image and create crypto image (CTI). For applying cryptography we select a small 64x64 image from the data set. This 64x64 image add any kind of information like account no, otp, password etc.

Figure 3: Shows the process of crypto Image

Cover image (CI)

Cover image is the image in which Crypto Image is hiding. The proposed work focuses on spatial domain. It means that secret data (SD) is hidden only in pixels. There are different type of cover image data sets that are available in the field of image processing. The proposed method uses a standard data set images.

Postern Image (PI)

Postern image is created or generated when the crypto image is embedded into a cover image. The output is the summation of cover image and crypto image and is known as postern image (PI).

Postern image is generated at the transmitter end (Tx) and flows in the communication channel (Internet world) like wide area network. This stego image is received at the receiver end (Rx). After the receiving of postern image ,the decoding process is applied and secret information is obtained.

In this part of proposed method ,the steps of implementation of proposed work are shown.

First step

In the first step, we will enter the information which we want to hide like Account No, OTP, and Password etc.

Second Step

In the Second step, we will select any small image i.e. 64x64 image from the database which is used to hide our information.

Third Step

After selecting the small image, small image is used for further processing of the proposed task of the image.

Select a window size 3X3 which is changed according to the pixel level.

Case 1

If 3X3 window contain all zeros and all ones, escape the window.

$$\text{Matrix} = \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

$$\text{Matrix} = \begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix}$$

Case 2

If all pixel contain different values then all binary data embed into these pixels.

$$\text{Matrix} = \begin{matrix} 212 & 73 & 145 \\ 149 & 193 & 19 \\ 140 & 192 & 13 \end{matrix}$$

Fourth Step

After generating the crypto image (CTI), now we will select the cover image from the data set and apply preprocessing task in this image. In the preprocessing of the image, some basic image processing operation will be performed in the selected image like gray scale converting, image resizing and other basic operations. This cover image (CI) is used to hide crypto image (CTI).

Fifth Step

After embedding the crypto image in the cover image we get postern image (PI). This is sent to the communication channel. After completing the "postern image", transmitter end process is completed.

Communication Channel

After creating the postern image, send this image in the communication channel. Before sending it into the communication channel apply zeros and ones padding on it. Zeros and ones padding work as a guarding for the postern image (PI) that is used to reduce the error probability in the image.

First Step

First collect the postern image from the communication channel. Select the collected "postern" image. Remove all the added zeros and ones from "postern" image.

Second Step

In postern image (PI),decoding process is applied. Check the pixel and select the LSB bit for data extraction from the postern image (PI).

Third Step

After decoding the Postern image (PI) we will get the Crypto image(CTI) and the secret information which is transmitted by the transmission end.

Fourth Step

Convert this binary information into the "String from or data from". Separate both the secret data and 64x64 small Image.

Fifth Step

After obtaining the secret data match the secret data of transmitter end.

Sixth Step

Calculate the quality check parameter of the cover image and "postern" image.

For quality measurement of the proposed work , different parameters are used. They are PSNR, MSE, SSIM and payload capacity of the image. These are some quality check parameter. After satisfaction of the quality check parameter , the visual result of proposed work is seen.

5. SIMULATION AND RESULT

The result of our proposed method for data hiding of gray scale images shown in this section, simulation of our proposed method and result calculation. We have done our proposed work with the help the MATLAB R2012b software and simulate our whole proposed methodology in graphical user interface (GUI). The performance of the proposed algorithm is tested for different gray scale images that is shown in below figure. Basic configuration of our system is: Processor: Intel (R) Quad Core (VM) i3–3110 Central Processing unit @, 2.40 GHz with 4GB RAM: System type: 64-bit Operating System. MATLAB based simulation result shows good PSNR value for stego image and better quality of stego image as compare to other method that is shown in table II. In the field of image data hiding, people normally have anxiety about the stego image, the payload capacity of the embedded secret information or data, and mean square error of the output that is distributed in a communication channel. These criteria can be evaluated by PSNR in dB, Payload Capacity in bits, BR in Bits/pixel (B/P) respectively. For calculate the similarity of the cover image and stego image calculate the structural similarity index measurement (SSIM) of the both images. Performance of our proposed method are quantitatively measured by PSNR, MSE, and payload capacity (PC) and SSIM values defined by:

Mean Square Error (MSE): The MSE measures the standard amendment between the actual image (X) and the noised image (Y) and is given by:

$$MSE = \frac{1}{N}\sum_{j=0}^{N-1}(X_j - Y_j)^2 \qquad (1)$$

X_j Shows the cover image

Y_j Shows the stego image

The MSE has been extensively used to quantify image quality and once used alone; it doesn't correlate powerfully enough with sensory activity quality. It ought to be used, therefore in conjunction with alternative quality metrics and perception.

Peak Signal to Noise Ratio (PSNR): The PSNR is computed as:

$$PSNR = 10\ log_{10}\frac{s^2}{MSE} \qquad (2)$$

The PSNR is higher for an excellent worth image and lower for a poor quality image. It measures image fidelity, that is, however closely the distorted image resembles the actual image. In our research work on the basis of our image size 255x255, we mentioned PSNR and MSE are as follows.

Structural Similarity Index Measurement (SSIM): The structural similarity (SSIM) index is a method for predicting the perceived quality of digital television and cinematic pictures, as well as other kinds of digital images and videos.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

Comparison of proposed method with other methods.

Payload Capacity (PC): The payload capacity shows the load data of the stego image. That give the information of the data load capacity of the image.

PC = string (size) / (wxh)

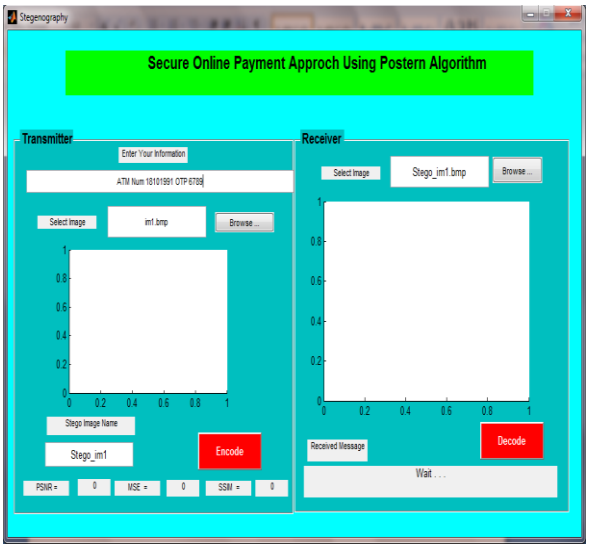
wxh – Shows the block size of the image.

These are parameters of result which is used to evolution of the quality of proposed work.

Figure 4 Shows the GUI of Proposed Postern Algorithm

Transmitter End

Step 1:
In the first step of we will enter the information which we want to hide like Account No, OTP, and Password etc**.**



Step 2:
In the Second step we will select any small image i.e. 64x64 image from the database which is used to hide our information.

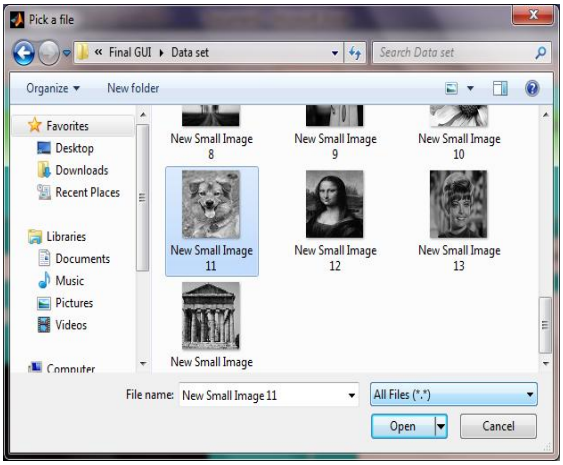


Figure 5: Shows the Small Media Image

After selecting the small image we will get the stego images which have secret information**.**

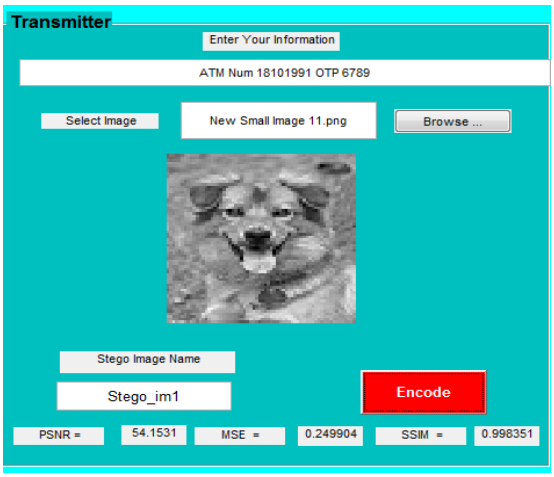
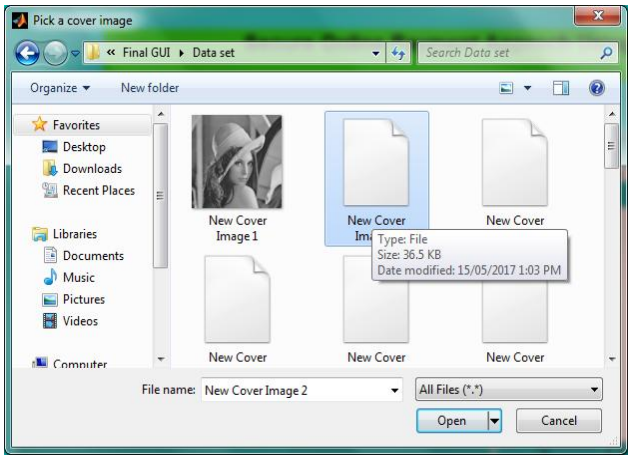
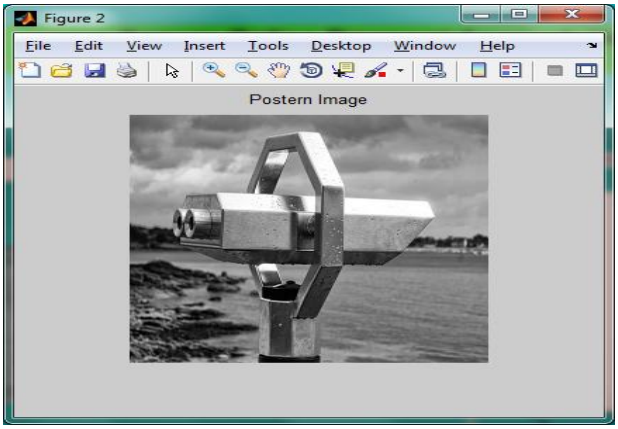


Figure 6: Shows the Crypto Image

Step 3:
In the third step we will encode the stego image and select a cover image in which we hide stego image.



After selecting a cover image we will get a postern image.



Receiver End

Step 1:

In the receiver end firstly we select the postern image which we get from the transmitter end.

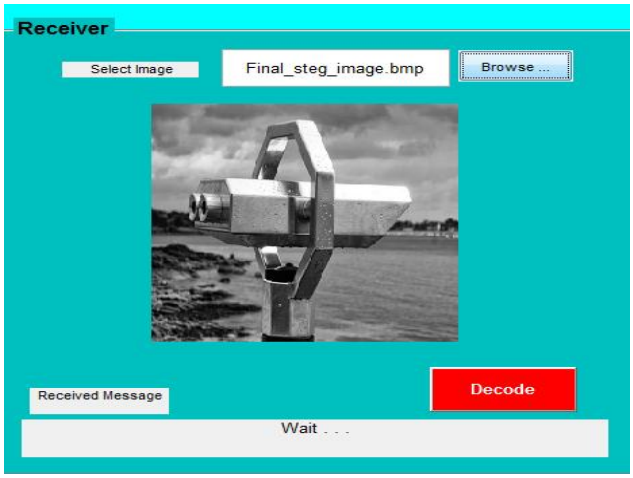


Figure 7: Select Postern Image

Step 2:

After selecting the cover photo we will decode the image. After decoding the cover image we will get the stego image and the secret information which we transmitted**.**

Figure 8: Output of the Receiver end

Table 1 shows the comparison of five different cover images with respect to the secret data that is shown in the above figure. The resultant parameters are peak signal to noise ratio, mean square error, and structural similarity index measurement is shown in below.

Data set of different images

(a) 64x64 New Small Image 1

(b) 64x64 New Small Image 2

(c) 64x64 New Small Image 3

(d) 64x64 New Small Image 4

(e) 64x64 New Small Image 5

Figure 9: Shows the Small Media Image Size 64X64

(a) 256 x 256Cover img.1

(b) 256 x 256 Cover image 2

(c) 256 x 256 Cover img 3

(d) 256 x 256 Cover img 4

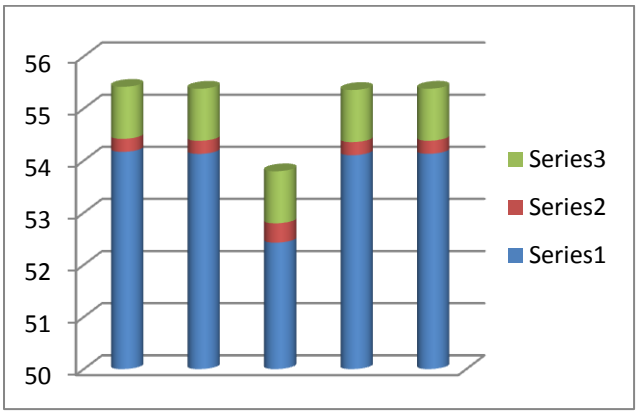
(e) 256 x 256 Cover image 5

Figure 10: Shows the Cover Image Size 256X256

Table 1 Shows the PSNR MSE and SSIM of different images

IMAGE NAME (64x64)	COVER IMAGE (256x256)	PSNR	MSE	SSIM
SMALL IMAGE1	COVER IMAGE1 (256)	54.1684	0.249023	0.998173
SMALL IMAGE2	COVER IMAGE2	54.1291	0.251288	0.998369
SMALL IMAGE3	COVER IMAGE3	52.4254	0.371995	0.997906
SMALL IMAGE4	COVER IMAGE4	54.1029	0.25281	0.999417
SMALL IMAGE5	COVER IMAGE5	54.1307	0.251196	0.997798

The table 1 shows the result in table after this shows in below figure. The compression of different images these are shown in figure 9 and figure 10. So finally the average PSNR of all images near about 55 dB shows good PSNR values. Also the good average of mean square error and structural similarity index measurement as per standard of images.



6. CONCLUSION

Digital Steganography is an engrossing scientific area which comes under the security system. In this paper, Steganography use based pixel identification and embed the secret data in postern algorithm. This concept enhances the security level since no one can extract secret data without having value of undefined region. The embedding gives high security as this is less sensitive to human eyes and also improves the quality of stego image. According to simulation results, proposed method provides fine image quality after hiding data in images. The output of our technique provides higher results because with the assistance of cropping, an increased security is provided by using postern algorithm. The proposed method shows good result as compare to other method in terms of PSNR (Peak-Signal-to-Noise Ratio), mean square error (MSE) Payload capacity (PC) and structural similarity index measurement (SSIM).

7. REFERENCES

[1] S.Adhikesavan and N.Sathish , “Steganography and Visual Cryptography for Online Payment System” , International Journal of Scientific Research Engineering & Technology, pp. 153-1603, March 2015.

[2] Ms. Nehashrivastavaand Prof. Mr. Toranverma, “A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency”, International Journal Of Advanced Research In Computer Engineering & Technology, pp.-1005-1009, March 2015.

[3] Souvik Roy and P. Venkateswaran, “Online Payment System using Steganography and Visual Cryptography”, IEEE Students’ Conference on Electrical, Electronics and Computer Science, 2014.

[4] K. Bennet, “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding information in Text,” Purdue University, Ceria Tech Report, 2013.

[5] Sumit Dhariwal and Sandeep Raghuwanshi, “ Content Based Image Retriveal Using Normalization of Vector Approach to SVM”, International Confrence on Computer Science, Engineering & Applications(ICCSEA 2012), May 25-27, 2012.

[6] S.Premkumar and A.E.Narayanan, “New Visual Steganography Scheme for Secure Banking Application,” Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumara coil, India, 2012.

[7] K. Thamizhchelvy and 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.

[8] ShengDun Hu and KinTak U, “A Novel Video Steganography based on Non-uniform Rectangular Partition”, 14th IEEE International Conference on Computational Science and Engineering, pp. 57-61, 2011 IEEE.

[9] Jaya, Siddharth Malik, Abhinav Aggarwal And Anjali Sardana, “Novel Authentication System Using Visual Cryptography”, pp. 1181-1186, 2011 IEEE

[10] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, “Visual cryptography improvises the security of tongue as a biometric in banking system,” Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.

[11] Jihui Chen, XiaoyaoXie, 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.

[12] KalavathiAlla, Dr. R. Siva Rama Prasad, “An Evolution of

Hindi Text Steganography," Proceeding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.

[13] ChetanaHegde, S. Manu, P. DeepaShenoy, K. R. Venugopal, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications," Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008.

[14] 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.

[15] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.

[16] 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.

[17] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[18] http://eprints.utm.my/38968/3/AliSalehAliAl-Ajam PFPPSM 2013CHAP1.pdf.