



Study On Secure Transaction Using Steganography And Visual Cryptography

¹Chethana N S

¹Senior Scale Lecturer, Dept. of ECE Government Polytechnic, Hiriyur, Chitradurga 577599, Karnataka, India

ABSTRACT

Information security has become the area of concern as a result of widespread use of communication medium over the internet. Security of data has become a most important issue in data communication specially in the field of computer networks. With ever increasing popularity of online transaction, debit or credit card fraud and personal information security are major concerns for customers, merchants, and banks especially in the case of card not present. This paper presents a survey about different fields where Steganography and Visual Cryptography can be used and a new method that uses a combination of Steganography and Visual Cryptography that provides only limited information required for fund transfer during online transaction.

Keywords: Data security, Steganography, Visual Cryptography, Online Transaction.

I. INTRODUCTION

With network growing rapidly, there is an urgent need to ensure information security in the present era of electronic commerce. Internet has become the primary source of transmitting confidential data such as military information, financial documents etc. online transaction is mainly used in online shopping. Online shopping is the act of purchasing products or services over the internet. The two most common problems of online

transaction are Identity theft and Phishing. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for purchasing. Phishing typically uses fraudulent email and fake websites to carry out fraud, deceived and victimized tend to reveal their financial data, such as credit card numbers, account user names, passwords and social security number and so on.

This paper presents a method that uses Steganography and Visual Cryptography, which reduces the information shared between consumer and the online merchant thereby enables successful fund transfer between the consumer and the merchant. This safeguards the consumer information and prevents misuse of information at merchant side. This approach is mainly used for E-Commerce but can be extended for Online as well as Physical Banking.

II STEGANOGRAPHY AND VISUALCRYPTOGRAPHY

Steganography is an art of hiding a secret message within an ordinary message and the extraction of it at its destination. Steganography takes Cryptography a step further by hiding an encrypted message so that no one suspects it exists. Ideally anyone scanning your data will fail to know it contains encrypted data. Text, Image, Video, Audio are used as a cover media for hiding data in steganography.

Visual Cryptography provides confidentiality without any cryptographic knowledge or complex computations. Visual information is encrypted by decomposing it into several images called shares, in such a way that decryption can be done by human visual system with stacking of shares.

III. RELATED WORK

Naor and Shamir [1] proposed a new cryptographic area called visual cryptography based on the concept of secret sharing. It divides an image into collection of shares and requires threshold number of shares to retrieve the original image. The decrypted message is obtained from stacking of

shares. The most notable characteristic of this scheme is to have a computation less decryption. It can also be used for applications which do not want to trust every participating entity in the process, using General Access Structure scheme. Another interesting extension of the original model is to generate innocent-looking shares so that attacker cannot get doubtful looking at the random pattern of the share. Visual cryptography is expanded to encode multiple secret images together so that overhead of keeping too many shares can be reduced. One other advancement in this field has been done to encode multi pixels in order to reduce the share size and make the performance better.

Katiyar S, MekaK.R., Barbhuiya F.A, Nandi S [2] used cryptography and steganography at the same time to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for steganography and as keys for cryptography. The key image is a biometric measure, such as fingerprint image. Proper use of cryptography greatly reduces the risks in these systems as the hackers to find both secret key and the template. The basic idea is to merge the secret key with the cover image on the basis of key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable to the human eye. The system targets the authentication requirement of a voting system.

Jaya, Siddhartha Malik, Abhinav Aggarwal, Anjali Sardana [3] designed a system to create two shares of customer image and signature. One image share and one signature share is printed on the card that is with the customer. The bank keeps remaining one image share and gives the second signature share to the central authority. Each customer is first validated against the reconstructed customer image for which the shares are with the user and the bank. If the generated image is identical to the user, next validation step is performed. If the validation fails, the customer is declared unauthenticated at this very step.

Chethana hedge, Manu S, P DeepaShenoy, Venugopal K R, L M Patnaik [4] presented a system where signature on the application form is considered as the input. The signature of the customer is scanned from the application form. This image is preprocessed to thicken the light shaded parts of the signature and to increase the intensity of the image. The preprocessed image is encrypted to get shares. The number of shares to be created is based on the scheme opted by the bank and the mode of operation of the account. Combining the shares a key share is created. Overlaying the share on each of the remaining shares will separately reveal two images. Thus, each customer can separately be authenticated and allowed to do transaction just by revealing his/her signature only. The shares are printed and handed over to customer, just like any credit/debit card. During further transaction customer has to produce his share. This will be overlaid over the bank's share to decrypt the image. After decrypting the signature, the post processing is done on the decrypted image. Finally the original image and post processed image are compared to confirm the authenticity of the customer.

SowmyaSury adevara, RohailaNaaz, Shweta, Shuchita Kapoor, Anand Sharma [5], proposed a tongue biometric authentication system. The customer needs to set in the location of the human head at the bank site. The system locates the user's tongue it takes a high resolution images by 2 digital cameras which contains both tongue texture and tongue shape and extract feature information from those images. These images are first processed and then to make it more secure we apply

visual cryptography on those images. Also a tongue code for each customer is made to identify each individual tongues. But use of biometrics is a drawback in this.

Souvik Roy and P. Venkateswaram[6] designed a payment method for online shopping by combining steganography and visual cryptography that provides customer data privacy and prevents misuse of data at

of customer authentication password. 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.

IV. CONCLUSION

In this paper a brief survey about different fields where steganography and visual cryptography is used are explained. Finally, this paper concludes that a combination of steganography and visual cryptography method can be developed to provide security to customer's data during online transaction.

V. REFERENCES

1. M.Naor and A. Shamir, "Visual cryptography, Advances in cryptology EUROCRYPT'94," in Lecture Notes in Computer Science. vol. 950, Springer, Berlin, 1995, pp. 1-12.
2. Katiyar S. Dept. of Computer Sci. & Eng., Indian Inst. Of Technol. Guwahati, India, Meka K.R.; Barbhuiya F.A ; Nandi S.
3. "Online Voting System Powered by Biometric Security Using Steganography".
4. Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, Indian

merchant's side. The payment system can also be extended to physical banking. In the bank, customer submits its own share and customer physical signature is validated against the signature obtained by combining customer's share and certified authorities share along with validation

Institute of Technology Roorkee, India., "Novel Authentication System Using Visual Cryptography".

5. Chethana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik Dept. of computer science and engineering, Bangalore University, India, "Secure authentication using Image Processing and Visual Cryptography for banking applications".
5. Sowmya Suryadevara, Rohaila Naaz, Shweta, Shuchita Kapoor, Anand Sharma Computer Science Dept. Mody Institute of technology, Laxmanghar Rajasthan India. "Visual Cryptography Improves the security of tongue as a biometric in banking system".
6. Souvik Roy and P. Venkateswaran Department of Electronics & Tele-Communication Engineering, Jadavpur University, Kolkata, India "Online payment system using steganography and visual cryptography".