Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018)
IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1

Secure Electronic Fund Transfer Model based on Two level Authentication

Vijay Kumar Sharma
[1]Computer Science and Engineering Department,
Manipal University, Ajmer Road,
Jaipur, India
Vijaymayankmudgal2008@gmail.com

Pratistha Mathur[2] and Devesh Kumar Srivastava[3],
[2,3]School of Information and Technology, Manipal
University, Ajmer Road, Jaipur, India
pratistha.mathur@jaipur.manipal.edu
devesh988@yahoo.com

Abstract—— **An Exponential growth of the high-speed internet has resulted in the rapid growth in online marketing. Online shopping provides the services to online shoppers as well as walk-in shoppers. However, security is the main concern in e-commerce in order to safeguard the confidential information, from online fraud, i.e. credit card or debit card fraud, leakage of information by the merchant or bank when a card is not used in online transaction etc. This paper proposed the two-way authentication technique modeled around visual cryptography and steganography techniques to protect the e-commerce fraud. The technique provides better security in term of authentication, identity theft and data transfer.**

Keywords— E-commerce; Steganography; Visual Cryptography; Phishing; Identity theft.

I. Introduction

Online availability of products fascinates users all around the world to shop online as it can be carried out from any location at any time. Many countries government around the world insists that each bigger money transfer should be in term of plastic money or electronic fund transfer (i.e. India). The main goal of the online market is to sustain the confidence between the buyer and seller which can only occur if the following things are considered:

1. The online shopping must offer good QOS (Quality of services).
2. The system should be highly secure.

Nowadays, security is a great challenge in the online system due to the technological advancement of attackers or hackers to breach the security, which was discussed by [1],[2]. In general two types of attack are possible in online shopping; these are phishing and identity theft as explain by [3],[4].

A. Phishing

Phishing is a type of criminal activity at online on social networking site which is started by an entity called Phishers. The phisher starts broadcasting email messages over the internet to the users around him and when the user opens these email they get re-directed to another website. The user thinks that the email has reached his or her inbox from some trusted party or bank. Hence, accidentally user furnishes all his personal details to the phishing attacker. They store this information in their database and misuse the confidential information of the user. In the year 2007, the bank or PayPal was the main target of these types of attackers, which was explained by [5], these types of attacks are mainly classified into following six categories as explained earlier by [6].

1. Malware phishing attacks
2. Deceptive phishing attacks
3. Pharming or phishing based on DNS
4. Man in middle phishing
5. Search Engine phishing
6. Content-Injection phishing

B. Identity theft

As the name suggests the fraudster steals the identity of a person. He or she determines additional possible ways to embezzle confidential information of the user, namely, e-mail address, personal address, fathers maiden name, place of born, bank A/C (account) details, pin number, and passwords etc. Using these data they steal the identity. It is one of the major problems in the United Kingdom, as explained in the special report on online fraud by [7]. To prevent the phishing attack and identity theft attack, visual cryptography and steganography techniques are used.

In this paper two level of the authentication process is applied first is based on visual cryptography (VC) technique and second is based on steganography followed by VC. Visual cryptography prevents the wrong use of information at merchant side because main aim here is to share minimum information in encrypted form, which makes the online shopping confidential as well as integral. The proposed method can be used for online banking, e-commerce, and physical banking.

II. Visual Cryptography

Visual cryptography was developed by Naor and Shamir. It was developed for protecting the secret of an image. VC based image encryption process divides original image into two or more shares (share is a binary image that cannot provide any information indivisibly), if image shares fall into wrong hand, it would look like as an image of random noise or bad art depending on the individual's experience. The shares are made by using two numbers 0 and 1. Number 0 represents the black pixel and 1 represents the white pixel. The combination of these shares generate the original image, the detailed study of VC is given in [8].

Steps of Encryption:

Step 1: Input image.

Step 2: Convert the image to binary image

Step 3: Generate two matrixes for storing share information.

Step 4: Create two share (share1 and share2) by using MATLAB randint function.

Decryption Process:

Step1: Apply OR operation on the matrix generated by share 1 and share2 and stores the result as

share=share1 OR share2;

Step2: apply 1↔0 on every pixel value in share and get output image.

Step 3: Stop.

III. Image Steganography in electronic fund transfer

Steganography is an art of hiding the features of the valuable documents. This technique is used for many decades now. It can be better choice for hidden communication or in other word we can say that image based steganography is better choice to stop fraud in e-commerce or online banking system. The combination of steganography with the visual cryptography makes it more resistant then other existing techniques. Many steganography techniques are available. Here, we are using haar (discrete wavelet transform) DWT based steganography technique.

Algorithmic steps for steganographic encoding is shown as follow

Step 1: Take two images one is the cover and other is secret image.

Step 2: Take one-level two-dimensional Haar discrete wavelet transform of the cover image.

Step 3: Apply a two-level two-dimensional Haar discrete wavelet transform of secret image.

Step 4: Extract approximation coefficient and detail coefficient of cover and secret image independently.

Step 5: uses the alpha blending on the resulted image from step2 and step3.

Step 6: do two-dimensional Haar inverse discrete wavelet transform to get stego image.

The decoding process is just reversible process of the encoding process.

IV. Transaction Process in Online shopping

In the conventional online shopping customer select, the items in cart and merchant's website direct him to an online payment page. Many online merchant systems take advantage of the services of third-party online payment system as Web Money, PayPal and many more. When the customer pays at online portal he or she submits his or her information in the form of card details, i.e. name and card number on the card, expiry date, CVV (Card Verification Value) no etc. In,[9] VC based technique is used to prevent password and signatures forgery. Figure 1 shows the flowchart of traditional online shopping system.

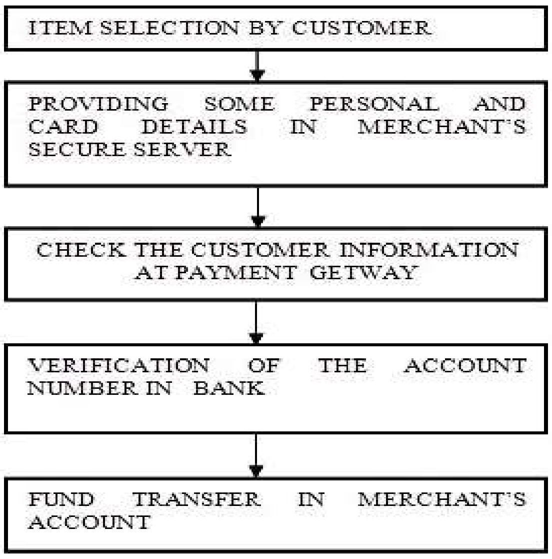

ITEM SELECTION BY CUSTOMER
PROVIDING SOME PERSONAL AND CARD DETAILS IN MERCHANT'S SECURE SERVER
CHECK THE CUSTOMER INFORMATION AT PAYMENT GETWAY
VERIFICATION OF THE ACCOUNT NUMBER IN BANK
FUND TRANSFER IN MERCHANT'S ACCOUNT

Fig. 1. Traditional online shopping

In, [10] the secure online e-banking system is presented, but here is one disadvantage that embedding process of the small message results in a larger message. So it is applicable only small message. In, [11], explained Advanced Persistent Threats (APTs) and there protection in online banking and in [12], also explained the need for security in online shopping

The information demanded by the many online shopper's systems for example; many demands PIN (Personal Identification Number) at IRCTC web portal, CVV number etc. so here is a greater risk to provide such important information. Many phishing attacks are possible in the case of new users; here there is a pressing demand to improve the way in which information is exchanged between two systems so that merchant or any employee can't misuse the information, to prevent the misuse of this information it is a need to communicate the information in encrypted or hidden form with user authentication which was explained by [13],[14][15].

V. Proposed Method for online shopping

The proposed system is based on the minimum information providing from the customer, for that system use authentication based encrypted information transfer. A customer has two shares for following authentication process.

a). Certificate Authority (CA) (Let's say the first authentication).

b). Bank-based (Let's say the second authentication).

These shares are provided at the time of registration from the authority (i.e. CA, bank).

Figure 2 infers the processing steps of secure online fund transfer stages.

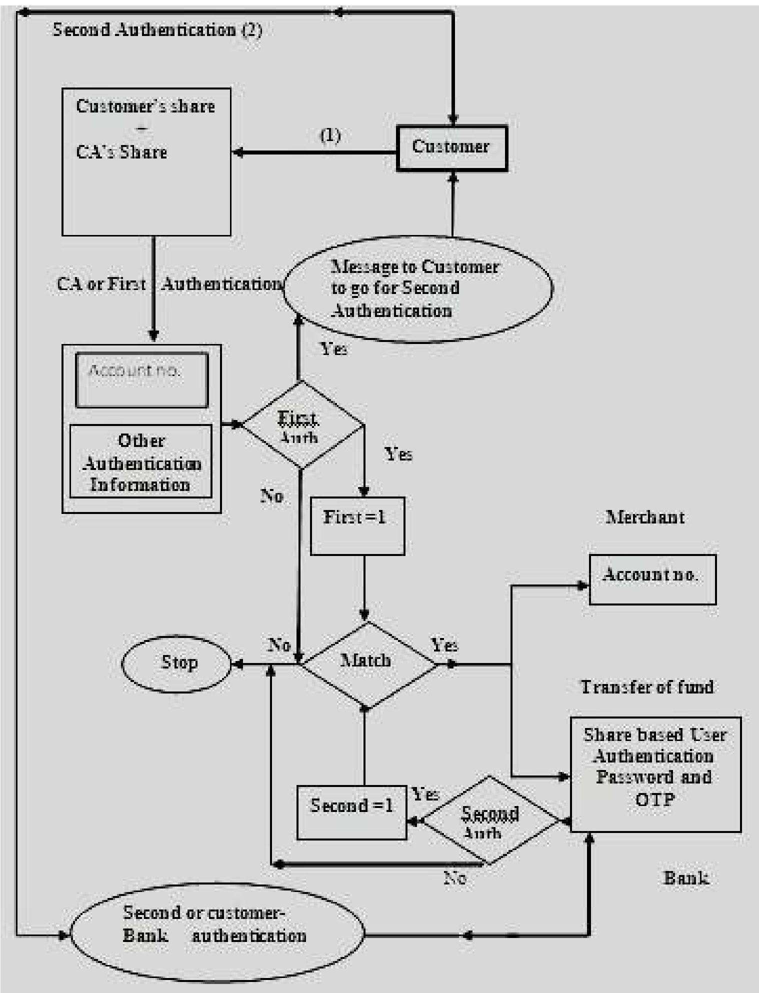

Second Authentication (2)
Customer's share
+
CA's Share
(1)
Customer
CA or First Authentication
Message to Customer to go for Second Authentication
Account no.
Other Authentication Information
Yes
First Auth
Yes
No
First=1
Merchant
Account no.
Stop
No
Match
Yes
Transfer of fund
Share based User Authentication Password and OTP
Second=1
Yes
Second Auth
No
Bank
Second or customer-Bank authentication

Fig.2. proposed online Processing Model for secure fund transfer

A. First authentication

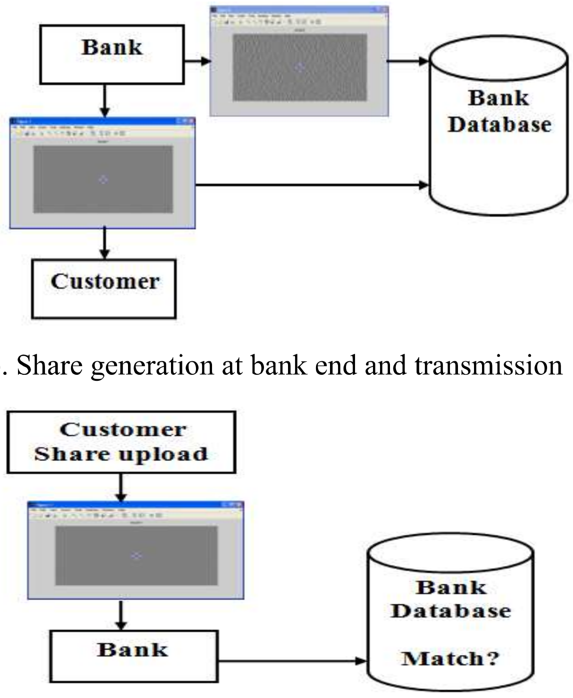
The first authentication takes place in between the customer and CA, for the security point of view CA is a highly trusted organization, which is authorized by the government of the respective country. In this authentication process CA use visual cryptography technique for share generation. It generates two shares, saves one share in his or her database for the first authentication and provides another share to the customer. This share is kept secret by the customer, nobody other than the customer has this share. During the first authentication, customer uploads a share at CA's portal. CA overlaps (decrypt) the customer share with its own share and generates an information image and in next step CA extracts information from this image and matches it with customer information which is present inside or CA's database. If a match occurs then do the following.

```
Set first=1;   and go for the second authentication
else
    stop
```

B. Second Authentication

From the security point of view, it is important to send the password in the encrypted or hidden form. The proposed method provides the total security related to password authentication which is based on the steganography followed by visual cryptography. To achieve it only single share is uploaded by the customer (say customer share). The customer share is provided by the bank to the customer when he or she registered him shelf or her shelf for the online shopping in the bank.

This share treated as the share of password at the banking end and banking side it overlapped with the share presented inside the bank database (bank share). Combination of bank share and customer share gives the image which is known as stego image. This stego image gives some related information about the user, but when the stego image is decoded it results from secret image or password image. Total password security is achieved by applying this process. The overall process for share generation is shown in figure 3 and 4.



a). Share generation at bank end and transmission

b). Matching process of customer share with bank share for password authentication

Fig. 3. share generation and matching in between customer and bank

The second authentication used share-based authentication (i.e. steganography followed by VC) followed by OTP (one time password) based authentication. In this authentication customer follow the following steps:

```
1.  Upload the customer share to bank
2.  Match the share inside the bank database or share present inside the bank.
3.  If match occurs then
        set second=1;
        and send OTP to customer;
    else
        stop
```

On the basis of first and second authentication process bank take the decision as:

```
if first = = second
 then
```

transfer the fund from customer's account to merchant's account.

Detailed view of share generation in second authentication process is shown in figure 4

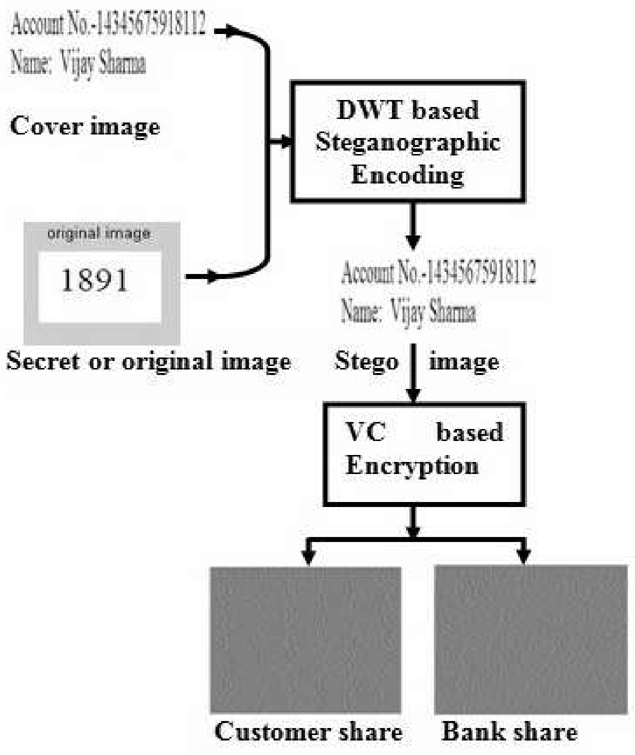


Fig. 4. Flow chart of the share generation for second authentication at bank.

Customer share is used by the customer at the time of second authentication process. At the bank's end, both shares are overlapped and generated the stego image. The stego image is again decoded and secret image or password is derived.

The above process is applied at the bank. Firstly, bank mixed original password image(secret image) with cover image (i.e. account number and name or may be other) and generate the stego image. This stego image pass through the VC based encryption. It gives two shares, i.e., bank share and customer share. Bank share is reserved by the bank and send customer share to the customer.

VI. Visual Advantage of proposed Method

Following are the main advantage related to security

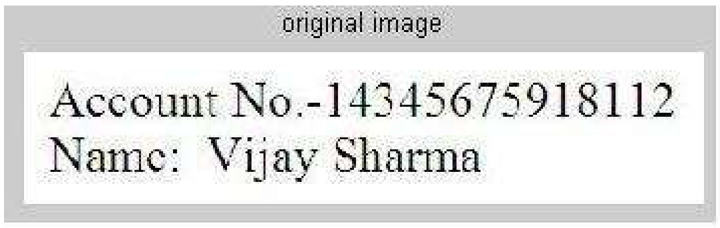
1. Leakage of secret information is protected because the main communication of secret information is in between customer, CA and bank, instead of customer and merchant.

2. Merchant portal transfer the shopper to CA's portal and the share-based authentication process is used in between CA and customer that increase secrecy.

3. The steganography and VC algorithm used at the bank side is free from third party involvement; there is no chance to extract the secret image or password image from the overlapped customer and bank share. Because bank provides only one share to the customer and kept another share in its database.

VII. Matlab results related to Extraction process

Figure no 5-8 shows the results related to CA and customer communication


original image

Account No.-14345675918112
Name: Vijay Sharma

Fig. 5. Snapshot of the original image

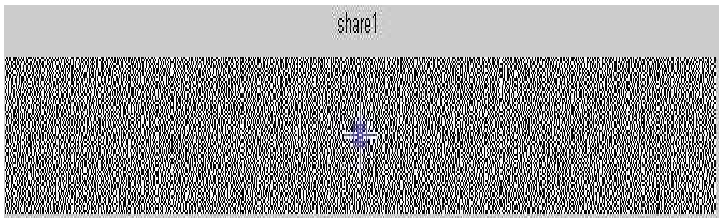


Fig. 6. Customer share

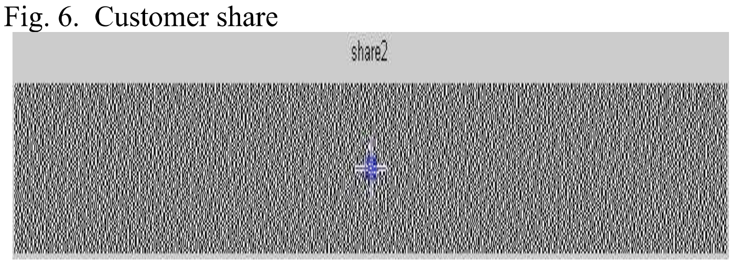
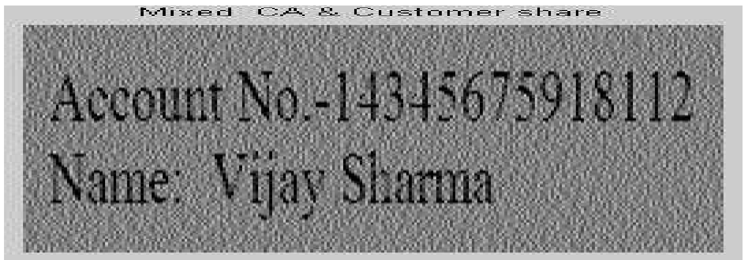


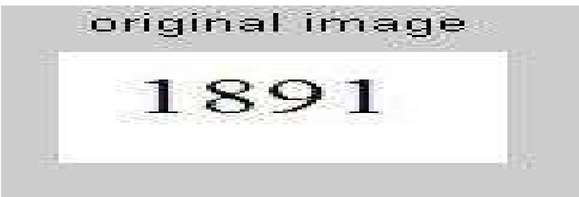
Fig. 7. CA's Share


Mixed CA & Customer share

Account No.-14345675918112
Name: Vijay Sharma

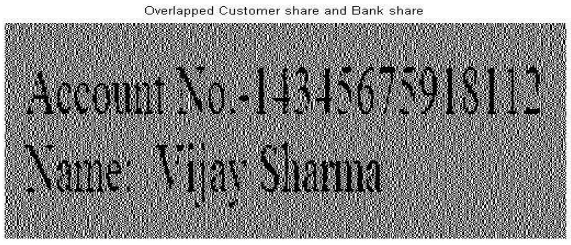
Fig. 8. Overlapped CA and customer shares

Figure 9 shows the original password image and result related to overlapped customer and bank related shares are shown in figure no 10.


original image

1891

Fig. 9. Original Password image at Bank


Overlapped Customer share and Bank share

Account No.-14345675918112
Name: Vijay Sharma

Fig. 10. Overlapped Customer share and Bank share for the second Authentication

This overlapped bank and customer share contain the password, on the bank side this image is treated as stego image and secret password image is decoded that gives the password image as the result as shown in figure11.

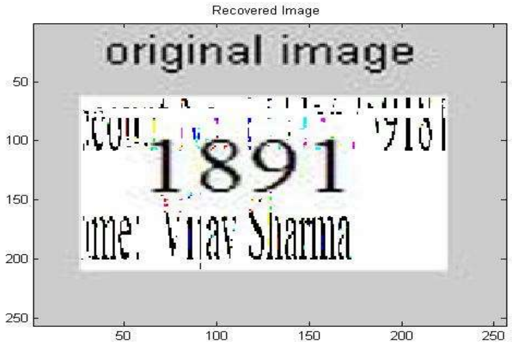


Fig.11. Secret password image derived from customer and Bank share.

VIII. Conclusion

Paper present secure online shopping system based on the application of visual cryptography and steganography. Visual cryptography-based authentication process protects the customer information theft as well as secure fund transfer. The proposed system can be implemented in e-banking as well as physical banking or other highly secure online fund transfer system. The use of steganography makes it highly secure and free from the most powerful attack in the online banking system because nobody knows the encoding and decoding process and its shares because this process is used at the banker end. The steganography technique used in this work is blind means there is no need to send the cover image to the bank.

References:

[1]. Daljit Kaur & Dr. Parminder Kaur,: Empirical analysis of web attacks. International Conference on Information Security & Privacy 2015, pp., 298-306, INDIA, (2015).

[2]. Saad M. Darwish & Ahmed M. Hassan,: A model to authenticate requests for online banking transactions. Alexandria Engineering Journal, vol. 51,pp. 185-191, (2012).

[3]. Navjeet Kaur,: A survey on online banking system attacks and its Countermeasures. IJCSNS International Journal of Computer Science and Network Security, vol. 15(3), pp. 57-61, (2015).

[4]. Hyoungshick Kim, Jun Ho Huh & Ross Anderson,: On the Security of Internet Banking in South Korea: a lesson in how not to regulate security'. Cambridge University Press available: http://www.cl.cam.ac.uk/~hk331/Publications/sp10KoreanBanking_v3.pdf (2011).

[5]. S. Manasa, P. Mullaimalar, G. B. Gnanaprakash Singh & S. S. Manivannan , "Securing Online Bank Transactions from Phishing Attacks using MFA and Secure Session Key. Indian Journal of Science and Technology, vol. 8, pp.123–126, (2011).

[6]. Markus Jakobsson & steven M.,: Phishing and countermeasures: Understanding the increasing problem of electronic identity Tehfts, Wiley-Interscience, A john Wiley and Sons, Inc., Publication, vol. 1, pp. 31-37, (2007).

[7]. Digital Thieves , A special report on online fraud by CIFAS, National Identity Fraud Prevention Week by The UK's Fraud Prevention Service 2010,"https://www.cifas.org.uk/secure/ContentPORT/uploads/documents/Cifas%20Reports/Digital_Thieves_October2010.pdf".

[8]. M. Naor & A. Shamir.: Visual cryptography. Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, (1995).

[9]. Chetana Hegde, S. Manu, P. Deepa Shenoy, 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,vol. 5(2), pp. 65-72, Chennai, India (2008).

[10]. Souvik Roy & P. Venkateswaran.,: Online Payment System using Steganography and Visual Cryptography . IEEE Students' Conference on Electrical, Electronics and Computer Science. Maulana Azad National Institute of Technology, Bhopal, India, (2014).

[11].Mohannad Alhanahnah & David W Chadwick., : Boosting usability for Protecting Online Banking Applications Against APTs, IEEE Cyber security and Cyber forensics Conference, pp.70-76, Amman, Jordan, (2016).

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

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

[14]. Himika Parmar, Nancy Nainan & Sumaiya Thaseen.,: Generation of secure one-time password based on image authentication. Computer Science & Information Technology, vol. 6(1), pp. 195-206, (2012).

[15]. Prakash Chandra Mondal, Rupam Deb & Mohammad Nurul Huda.,: Transaction Authorization from Know Your Customer (KYC) Information in Online Banking. 9th International Conference on Electrical and Computer Engineering, pp. 523-526. Dhaka, Bangladesh, (2016).