Avoidance of Unauthorized user using Visual Cryptography

Dayanand G Savakar¹, Pandurang H Biradar²

¹Rani Chennamma University, Belagavi
²BLDEA”s Vachana Pitamaha Dr. P.G.Halakatti College of Engg. & Tech, Bijapur

Abstract: This Work makes use of divide and conquers algorithm and visual cryptography method. The use of visual cryptography is to protect bank account from hackers using image as security. The original image will be added at registration process then it divide into two parts, first part share with server and second part share with registered email id. Whenever we need to transfer the money from bank account to another then we need to upload second half image it will merge both parts if it matches. The money will transfer otherwise Transaction will unsuccessful. Finally it shows authorized user can perform activity on their account. Avoid the unauthorized user access.

Keywords: visual cryptography, security, shares, divides and conquer algorithm, hackers

1. Introduction

Online transaction is nowadays become very common and there are various Security Issues Involved in doing it. Referring this Work we can protect personal and bank account information. This Work consists of two parts. One is visual cryptography another is dividing and conquers method. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Here image will divide and generate two images, at the end it combines both of them and compares with original image, if it matches then he/she is authorized user.

Firstly user wants to avoid the unauthorized access and protect accounts of e-commerce and bank account. User need to register the application with specified information and uploading image for security purpose then it divide into two parts, first part share with server and another will share with registered user email id. After to login the page to buy a product then they can search product and finally user can buy registered user email id. After to login the page to buy a product then they can search product and finally user can buy.

Drawback of Existing System

1)Delay in delivery: Message delays plague SMS services. Once sent out, an SMS OTP traverses multiple hops across carriers. It becomes susceptible to delays caused by network congestion. 2FA OTPs being time sensitive (typically three to five minutes), OTP delays can lead to “session time-outs”. Operator service outages and gateway downtime also affect SMS-based OTPs.

2)Government/regulator interference: The Indian government has set precedents for blocking bulk-SMS gateways for law and order purposes. This is a serious concern for online banking services dependant on SMS-based OTPs. For example, one of India’s largest PSU banks once had to contract a Bangladeshi SMS gateway to send out its OTPs. This increased its cost by 100% at Re. 1/SMS.

3)Low level of security: In India, the SMS encryption in use is usually basic in nature. SMS-based OTP also adds several variables to the trust chain. If a gateway is compromised, it will result in a major security breach, especially when it involves overseas gateways. SIM cloning is another emerging threat vector for SMS-based OTPs, with documented cases of frauds in India rising.

4)Coverage areas/unavailability of service: Since SMS-based 2FA OTPs are sent over the air, users outside the network coverage can face issues. When users travel abroad, there are restrictions on incoming SMSs.

5)Unavailability of devices: The user’s registered mobile device needs to be physically available to be able to receive the SMS OTP.

6)Cash on delivery: Still some shopping carts prefer cash on delivery because they are not supporting internal security and banking system to transfer money.
2.3 Proposed System

Our goal of proposed system is to raise the security level and to prevent the user accounts from frauds. By using visual cryptography technique and also one secret code. In this technique we are using one picture at the time of registration then using divide and conquer method to divide the picture into two shares one share will be in server side and another share will send to user email id. Whenever user buying product then need the user side second half share to upload this picture then compares combined picture with original picture if matches then only transaction will happen.

This technique is safe and security level is high because there is no need of any cards and its information. Directly we can link to the user bank account. If the fraud saw the user image then also we cannot hack the bank account and security level is high.

User can protect the accounts and easily buy the products from e-market.

3. Process

![Diagram of E-Commerce Authorization Process](image1.png)

**Figure 1:** Managing the E-Commerce Authorization Process.

Our Work is on e-commerce process. In this process we need electronic product as computer and internet. In this application there we need to view the products easily and to select it and goes to payment method before that the security level will come. In this level only we are checking authorized person. If authorized person is confirmed then only permission to link the bank account otherwise it will not link bank account.

4. Flow of Application

![Flowchart](image2.png)

**Figure 2:** New User Registration screen

Registration page
Uploading the image in registration process then it will divide into two parts one will store in server side and another will send to client mail.

5. Screenshots
Confirmation page
Here to upload the client image which we got from email. To match with server image, if both matches to registered image then transaction will happen from bank account.

Purchased product page
After completion of security level the transaction will happen and to proceed to purchased product details page.

6. Conclusion
In this paper we proposed an effective technique to provide greater security in the field of Internet banking system by restricting the unauthorized user. It is the super concept to avoid the hacking. In olden days this concept was used in manually for example in the old films any items are buying in big amount then they need provide a proof for the person he/she taking the product, to verify the same by giving note or image will be broke into two parts and one will have buyer another will have seller, after meeting they need check it if it matches then item and money will be exchanged otherwise not. Based on this concept we did this application.

It’s useful to customers, website holders and banks. Image will divided, first half send to customer and second half of image will be kept in bank server.

In future enhancement this can be extended to signatures. Here image are taken as inputs since they are uniquely identified, but according to the user and bank convenience any kind of images can also be used like signature image of the applicant.

References
[9] BS Anami, DG Savakar, A Makandar, PH Unki (2005), A neural network model for classification of bulk grain samples based on color and texture, Proceedings of International Conference on Cognition and Recognition

Volume 5 Issue 8, August 2016
www.ijsr.net
Licensed Under Creative Commons Attribution CC BY