EMPLOYABILITY OF VISUAL CRYPTOGRAPHY IN ENHANCING THE SECURITY FEATURES OF ONLINE TRANSACTIONS IN THE E-COMMERCE FOR FORMAT

Atul Kalkhanda

ABSTRACT

In the last decades, E-commerce has taken the world literally by storm-there is hardly any domain left untouched by this rapidly growing medium of trade and commerce. The expansion of E-commerce has, in turn, compounded the growth of fulfilling transactions using online banking or credit/debit cards. This would lead to the phishing of personal information if the security measures used on the payment gateway were not adequate. To overcome this issue, this research paper proposes a visual cryptography technique to make these transactions more secure.

1. INTRODUCTION

The process of buying products through web browsers referring to E-shopping instead of using mortar stores. No clients on the web have exponentially expanded step by step; this development has given a significant extension to internet shopping. Internet shopping is fundamentally a procedure to check, feel, and request the huge number request of items accessible for sale by the online retailers. We need to choose the item on the online retailer's site, it will create the advanced buy request, after this we need to give the credit or plastic subtleties, and the item you have chosen will be conveyed to you via mail request or home conveyance by dispatch. E-instalment framework is an elective clarification given to the client to have a cashless exchange income back to the administrations/buy done. We can say that e-installment is a gadget by which clients can make Online Payments for his/her buy of useful things or administrations without the physical exchange of money and checks, independent of time and area. It is the premise of online installments, and online installment framework advancement is a higher type of electronic installment. It makes electronic exchange accessible 24*7 utilizing a web system to help web-based businesses. Data fraud and phishing are the real downsides of web-based shopping. Phishing is an amateurish method to take the end clients individual just as banking information. Some specialized experts are utilized to hack this information from online retailers with the goal that they can abuse this information. Wholesale fraud is a demonstration of taking and accepting someone else's character to carry out extortion or different violations like utilizing this information for obtaining or opening new financial balance. To ensure the taking of information between end clients and online shipper sites, we need to utilize Secure Socket Layer (SSL) encryption; this encryption ensures that the information will be epitomized and burrowed so that during the exchange it cannot be hacked. Still, this information will be accessible with the retailers, so we have to trust the workers of online products for not sharing the information or utilizing this information for their utilization. We are proposing another technique for this.

In this paper, the proposed strategy utilizes visual cognizance by literary bases, access to in any event data, and correspondence among customers and individuals from the commission. On the off chance that this data is ensured by the client and by the client, it is likewise given by the client data. The proposed substance is especially intriguing for an internet business, yet it is generally stretched out for web-based banking. The remainder of the paper is composed as pursues: Section II gives a brief portrayal of visual cryptography. Segment III contains a writing review. Area IV displays the present system for e-installment was done. Area V gives the proposed installment technique. Segment VI finishes up the paper.

2. VISUAL CRYPTOGRAPHY

Naor and Shamir suggested a new idea of visual cryptography (VC) in 1994. Visual cryptography, a developing cryptography method, uses the features of human visualization to decode the encrypted images. It involves neither cryptography information nor complicated calculation. For protecting purposes, it also protects that hackers cannot identify any hints about a secret image from separate cover images. The essential knowledge is to divide the data into n parts recognized as the shares. Only when an appreciation of the number of shares is stacked composed will human eyes identify the image content. Visual cryptography protects secrets inside the images. The image is distributed into several shares and later decode without any computation. This decoding is done by overlapping the shares, which will expose the secret image or text by the human visual system. At the beginning of the model, which was established, involves a ciphertext and a page of transparency. The introductory text is recovered by overlapping the transparency with the critical bygone of the ciphertext. More recently, this model is enlarged with k from a secret sharing pattern, where secret sharing is a method where secret shares are scattered between the participants. Thus, the secret can only publish when an appropriate number of shares are stacked together. The (k, n) secret sharing scheme exposes a secret image only when k or more thank shares are arranged.

However, share fewer thanks will not expose any information. In secret sharing method used a combination of black and white pixels in image and text. These white and black pixels show in n converted version called shares. Each share contains a collection of black and white subpixels. Examine visual cryptographic scheme: White pixel always produces one black and white subpixel after superimposing; however, loss pixel results in two black's subpixels. When shares are stacked collected, if the number of subpixels is more than the stable threshold, then that pixel is measured as "on" if it less then stables threshold it is measured as "off." It represents in Figure.1.

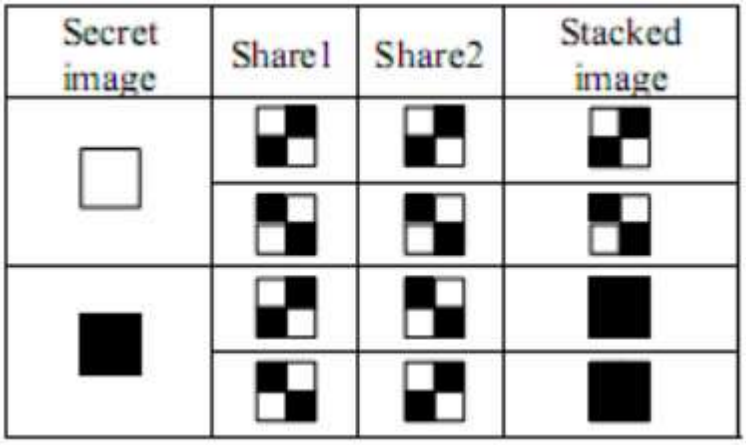

Fig. 1. Construction of (2, 2) VC

3. LITERATURE SURVEY

V Hemanth, M Shareef, and KS Ranjith in "Anti-Phishing use Visual Cryptography" in this paper received a result for anti-phishing with the use of visual cryptography. The online banking system uses visual cryptography to enhance security. By implementing the visual cryptography method, the phishing attack can be excluding. Analyze how to phishing attacks arise and how to determine an E-mail is a blackmail. B. Srikanth, G.Padmaja, Dr. Syed Khasi, Dr. P.V.S.Lakshmi, and A. Haritha proposed a technique where the mark of the candidate will be utilized as info and this information will be separated into a number of offers relying upon bank conspire. One offer will be kept with the bank, and every single other offer dependent on the plan will be given to the candidate. During each exchange, the candidate needs to supply his offers. These offers are covered with the offer present in the bank. Furthermore, an Authentication check is performed utilizing the connection system. In the event that the connection coefficient worth is higher than validation is succeeded. Souvik Roya, P.Venkateswaranb, presents an alternate way to deal with the English content-based steganography with Indian root. In the proposed technique, Resources of sentences are not utilized, rather properties of English language like utilization of periphrases, articulation, and fixed word requests are utilized. This gives us the capacity to perform sentence creation yet increments multifaceted computational nature adaptably. Souvik Roy and P.Venkateswaran Provided another methodology where restricted data should be shared for the cash move process while doing web-based shopping. End client's individual information is additionally kept from wholesale fraud. They have utilized steganography and visual cryptography for this reason.

S. R. Navale, S. S. Khandagale, R. A. Malpekar, Prof. N. K. Chouhan utilizes a content-based steganography and RG-based Visual Cryptography to master present on secure online installment framework where a buyer the installment data will be sent legitimately to an installment entryway and vendors are not accepting a customer installment data, additionally encoded/hashed form. 3.1. Similar Analysis In this paper, we think about various strategies that work on the online exchange, so examination sees in underneath table 1.

Table 1 Comparission Analysis

Sr. No.	Name of Paper	Method	Advantages	Disadvantages
1	A Text based Steganography technique with an indian root.	Vedic numeric code.	Flexibility and Freedom for sentence creation	Increases computational complexity.
2	Authorization of the medical bank of the process of image processing and visual representation.	Authorization of the medical bank of the process of image processing and visual representation.	This technique shield the customer information to defend the possible forgery.	Need physical presence of applicant to sign an application from while opening a bank account.
3	Online Payment System using Steganography and Visual Cryptography.	Vedic numeric code and Traditional Visual Cryptography.	Prevents unlawful use of customer's data on merchant side.	Meaningless shares are generated and transmitted over an untrusted communication channel.
4	Approach for Secure online transaction using Visual Cryptography and Text Steganography (Proposed Method).	Text Steganography using Ascii code and RG based Visual Cryptography.	Customer privacy is prevented from CA as well as Merchant. No pixel expansion while creating shares.	Lower Visual Quality.

4. CURRENT METHODOLOGY

In the current scenario, there are mainly three entities involved, namely Customer or Client, Merchant server, and Bank Server. The task of Customer or Client is first to make an account at the merchant server. The client needs to fill username, password, e-mail address, residential address, credit card details, and other confidential information in order to login to the merchant site. After the login is successful, the Client will select a product which he/she wants to purchase. After making a request to purchase a product, the Merchant server will send this information to the Bank server. In turn, the Bank server will send OTP to Client in order to authenticate the request raised by Client. At the client-side, OTP is validated, and the purchase order is placed. This OTP is valid till 10mins. When the Client is logged in, sensitive information such as credit card details can be captured by the attacker, or the site can be a phishing website.

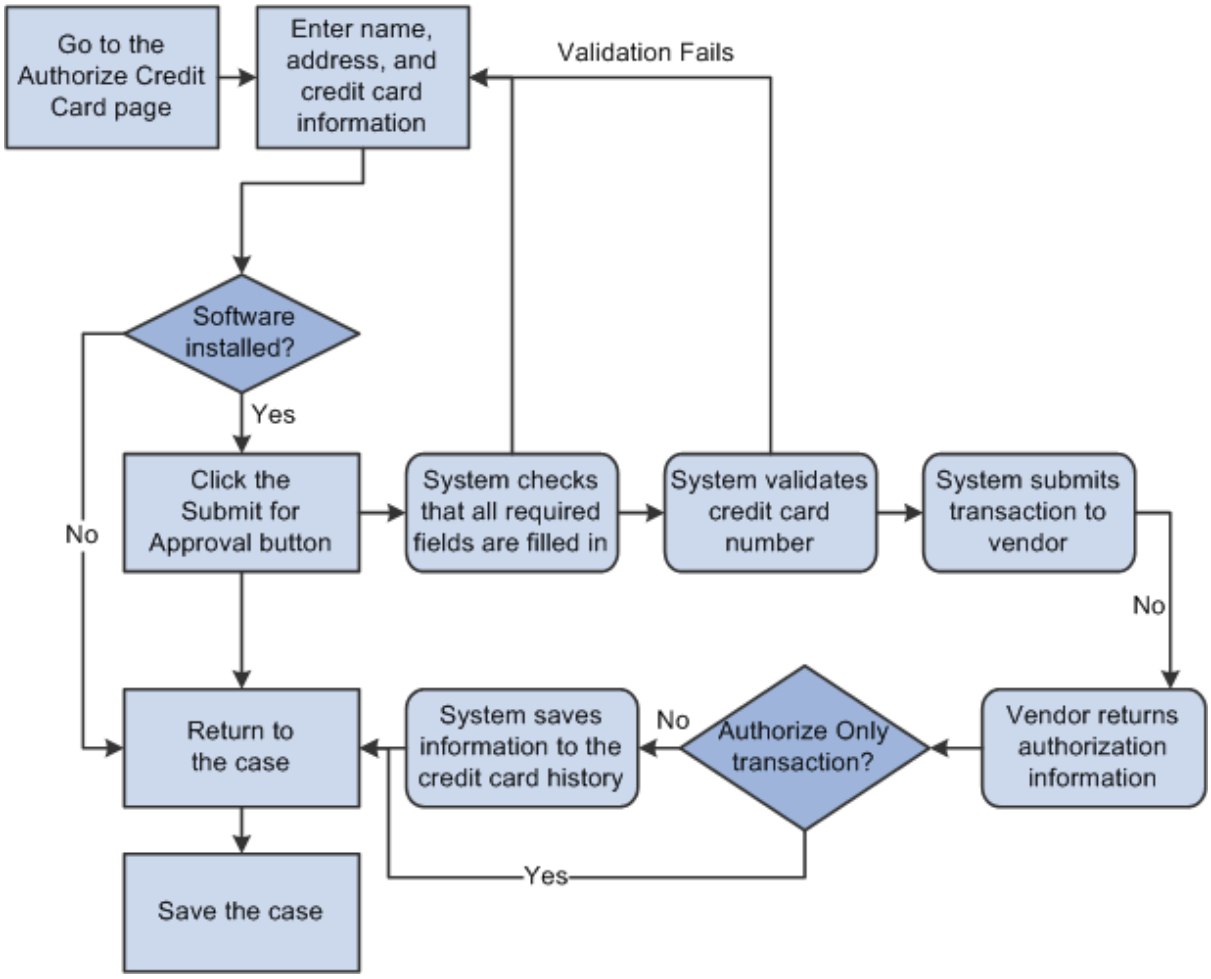

Fig 2: Existing System of E Payment System

5. PROPOSED SYSTEM

In order to purchase any goods, the customer needs to fill his/her confidential details at the Merchant site, but the customer doesn't know whether the merchant is genuine or not. So In proposed e-payment method will share minimum information to the merchant. The proposed method includes three main characters for online transactions: customer, bank, merchant, or retailer. Before purchasing online, the customer must open a bank account by providing his personal details to the bank. When the customer opens an account in a bank, the bank will give a private key, and this private key divided into two shares. One share will keep the bank in its database, and other shares will give to the customer. The version is created by applying visual cryptography to a snapshot of a text containing the customer's account number and debit and credit card information. By using these shares, customers can perform secure e-shopping. In Figure 3, Figure 4, Figure 5, and Figure 6 See how the share is generated, and the customer sees his / her personal information when the shares overlap.

Account no: 563214598965412

Name: Somil lohani

Fig 3: account number of User

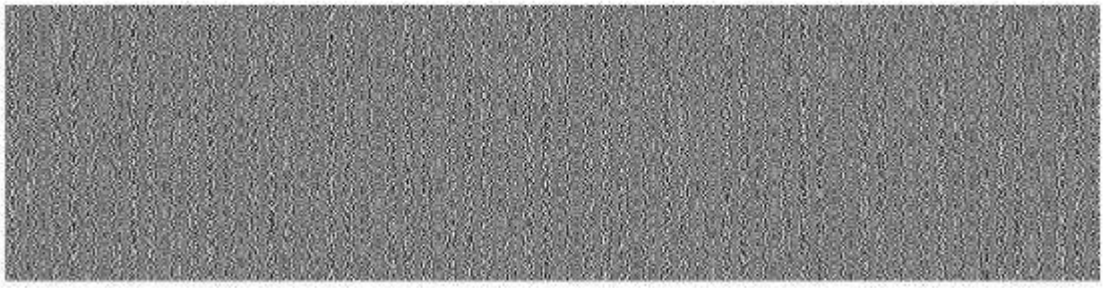

Fig 4: First part is in Client

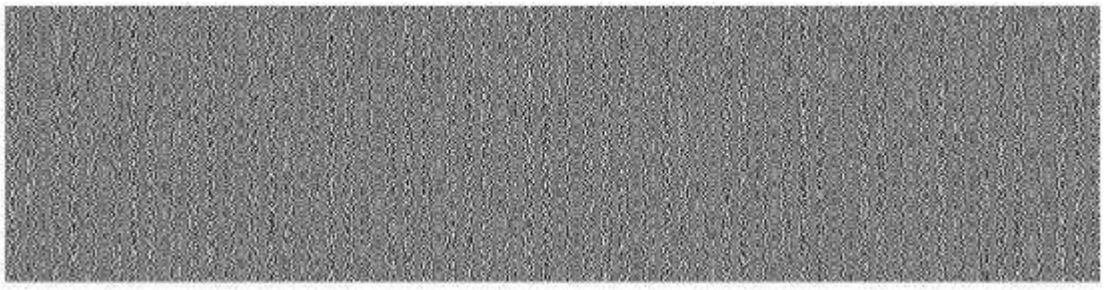

Fig 5: Second Part is with Bank

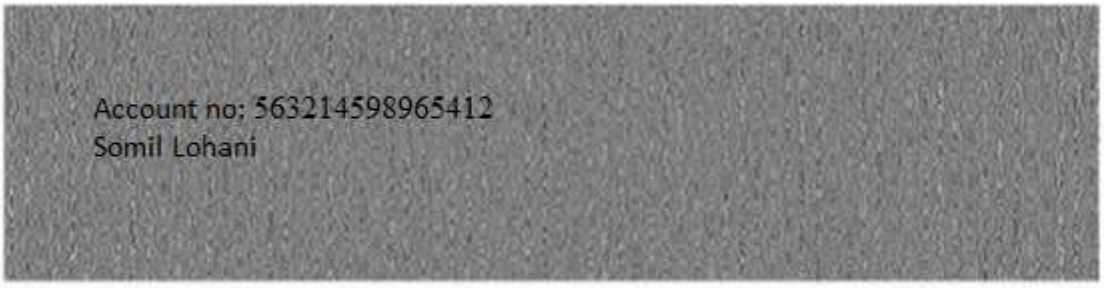

Fig 6: Data hiding in pixels of image

Figure.7 represent steps that needed in proposed system. In proposed method first customer open account in bank after bank will generated private key and that key will have divided into two shares. One share given to customer and second share keep bank in its database. When customer do online shopping he/she select item and add to cart then last they perform payment. Customer send his/her personal information to Merchant and merchant will send that personal information to bank. Bank have overlapping share1 and share2 and get personal information and bank verify that information then finally payment has processing.

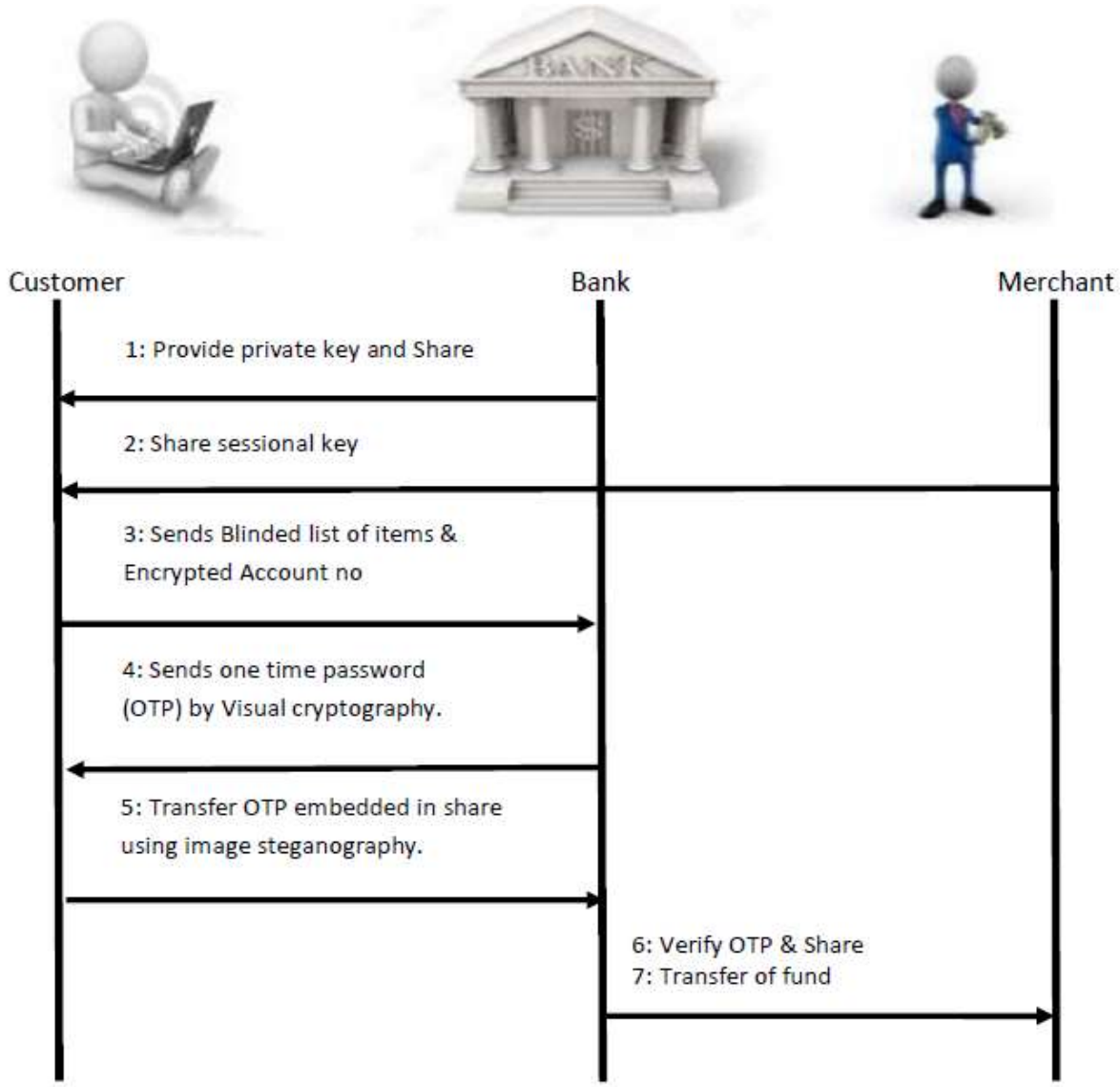

Fig 7: Proposed System

6. CONCLUSION

With the increasing cashless world, problems of secure transactions get up. Because of that, to help the customer while doing shopping through online retailer's website there is always a possibility of intrusions & personal information escape. During the said process vital information like bank details and customer personal information can be hacked and misused. Proposed method is presented to protect customer from phishing website and avoid misuse of the credentials. Hence the system will provide more secure online transactions by using visual cryptography