International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

Separable Information hiding by Embedding Keys

Hariharan M[1], Chandramouli A[2], Pradeepkumar J[3], Elakiya R[4]
[1], [2], [3] U.G. Scholar, [4] Assistant Professor Department of Computer Science Anand Institute Of Higher Technology, Chennai ,TN ,India.
[1]hariharan431@gmail.com, [2]acmouli25@gmail.com, [3]pradheepkumar.j@gmail.com, [4]elakiya1917@gmail.com

Abstract — **A rising in E-Commerce market is seen in recent time throughout the globe. With ever increasing quality of on-line searching, Debit or mastercard fraud and private data security area unit major considerations for purchasers, merchants and banks specifically within the case of CNP (Card Not Present). This paper presents a replacement approach for providing restricted data solely that's necessary for fund transfer throughout on-line searching thereby safeguarding client knowledge and increasing client confidence and preventing fraud. the tactic uses combined application of Modified Steganography and visual cryptography for this purpose.The proposed method aims at encrypting a JPEG bitstream into a properly systematic structure, and a secret message is embedded into the encrypted bitstream by modifying the JPEG stream. Usable bits suitable for data hiding is identified so that the encrypted bitstream carrying secret data can be decoded correctly.The cofidental message bits are encoded with error correction codes to achieve a data extraction and image recovery. The encryption and embedding are managed by encryption and embedding keys respectively.**

Index Terms — **Encrypted image, image recovery, information hiding,JPEG, reversible data hiding.**

I. INTRODUCTION

Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase,stuffing of credit or debit card information and shipping of product through mail or home delivery via courier.Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards.Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumer's personal identity data and financial account credentials..Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.In this paper, a advanced method is proposed, that uses text based steganography and visual cryptography, which reduce sharing of information between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side[10].As JPEG is widely used, in this correspondence we propose a novel RDH framework to hide data in an encrypted JPEG bitstream.The scheme is defined to perturb the principal content of the original image while preserving the bitstream structure. The secret bits are encoded with error correction codes and then embedded into the JPEG bitstream.On the receiving side, blocking artifacts of neighboring blocks are used to extract the secret bits and perfectly restore the original bitstream[1].

I. EXISTING SYSTEM

In this modern world, hackers use many techniques to break e-banking security. The latest security threats facing e-banking authentication systems are: Phishing trends, such as spear phishing ,pharming ,whaling and fast-ux service networks.Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumer's personal identity data and financial account datas.Payment Service,

Financial and Retail Service are the most targeted industrial sectors of phishing attacks[4].

Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However,one must still believe merchant and its employees not to sell the information to others and not to use consumer information for their own purchases[2].In order to hide four letter word, eight words are required prohibiting the words that are added to provide flexibility in sentence construction. So to hide a immense message, this technique requires large number of words and creates a difficulty in sentence construction[3].Disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information.

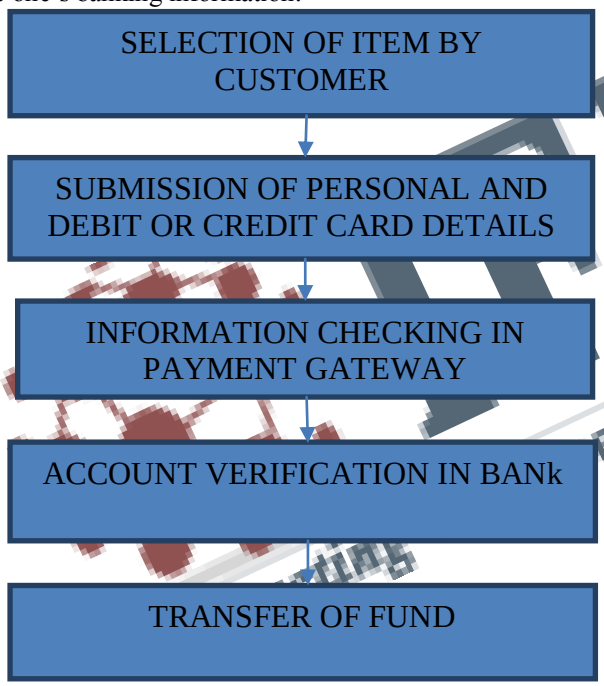


Fig 1.Existing System Architecture

II. System Structure

A. *Online Shopping System*

In traditional online shopping as shown consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, payonlinesystem, WebMoney and others. In the payment portal consumer submit his or her creditor debit card details such as credit or debit card number, name on the card, expiry date of the card. Details of information sought from shopper vary from one payment gateway to another. For example, payment in IRCTC website requires Personal Identification Number (PIN) when paying using debit card whereas shopping in Flipkart or Snapdeal requires Visa or Master secure code. In addition to that merchant may require a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard), which is basically an authorizing code in CNP transactions. According to the PCI Data Security Standard, merchants are prohibited from storing CVV information or PIN data and if permitted card information such as name, card number and expiration date is stored, certain security standards are required. However recent high profile breaches such as in Epsilon, Sony's PlayStation Network and Heartland Payment Systems show that card holders' information is at risk both from outside and inside. A solution can be forcing merchant to be a PCI complaint but cost to be a PCI complaint is huge and the process is complex and time consuming and it will solve part of the problem. One still has to trust the merchant and its employees not to use card information for there own purposes.

B. *Transcation framework*

The general framework of the proposed scheme is shown in Fig. 2.Consider three parties in the entire workflow of encryption embedding extraction restoration: *content owner*, *data hider*, and *receiver*, roles of them are described as follows.

Content owner: Parse the original JPEG bitstream and encrypt the bitstream to conceal the principal content of the originalimage.An encryption key is chosen by the content owner.The encrypted bit stream must have the same structure as the original so that it can be decoded correctly to give an undistorted.

Datahider:Embed the secret message intothe encrypted JPEG bit- stream. Suitable positions for data hiding are chosen, and the achievable embedding capacity calculated. Encode plain bits into secretbits with error correction codes (ECC)[7]. The word plain is associated with the original message to be transmitted, and secret corresponds to the ECC-encoded and encrypted secret bits.An embedding key is usedby the data-hider for security.

Receiver: Extract the secret message and recover the JPEG bit- stream. With both the encryption key and

embedding key, the secret bits are extracted and decoded into plain bits, and the original JPEG bitstream is perfectly restored. If the receiver only has the encryptionkey,an image with good quality can still be obtained approximately. Generally, these RDH methods are useful for embedding data into images that are open to the data hider.In some applications,the image owner may not be willing to disclose the image contents to the data hider[9].For example,the patient's private information must not be revealed to the person who embeds data into the medical image, while the original image must be recovered perfectly and embedded data completely extracted on the receiver end[5].

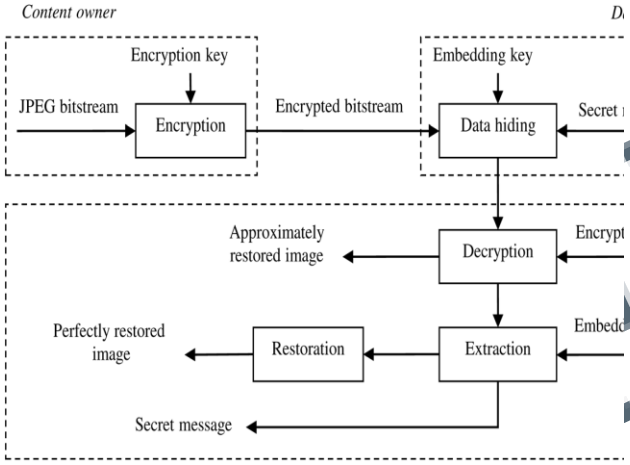


Fig. 2. Sketch of the proposed framework.

IV. BITSTREAM PARSING AND ENCRYPTION

A. **JPEG Bitstream Parsing**

According to JPEG standard an image is decomposed to a set of quantized DCT coefficients in non overlapped blocks,and then coded into a bitstream with entropy encoding.During entropy encoding, the DC coefficients and the AC coefficients are handled separately. The DC coefficients are coded with the Huffman codes after using a one-dimensional predictor Bitstream parsing is a part of the entropy decoding, which analyses the compressed bits according to the JPEG structure and the Huffman tables extracted from the JPEG file header.

B Bitstream Encryption

We aim at encrypting a JPEG bitstream into the one that can be decoded into an unrecognizable image directly by a JPEG decoder.Due to the strict structure of JPEG data, any alteration on individual bit may cause the failure of decoding. Therefore, special care is taken in the present work to devise a JPEG encryption scheme. For that purpose, we do the encryption according to the encoding structure by selecting and modifying the changeable bits.The encryption procedure consists of two steps, encryption of the appended bits and encryption of the quantization table.

V.DATA HIDING IN ENCRYPTED BITSTREAM

A. **Locating Appropriate Embedding Positions**

When the data hider receives the encrypted bitstream, although the data hider does not know the contents of the original image, additional data can still be embedded into the image by modifying some bits.An example given in which the dark blocks are used for data hiding, and the shaded blocks skipped. It should be noted at this point that, to embed data, it is unnecessary to decode the bitstream into an encrypted image. Nonetheless, for easy description in the following, one might imagine there were an encrypted image decompressed from it[8].

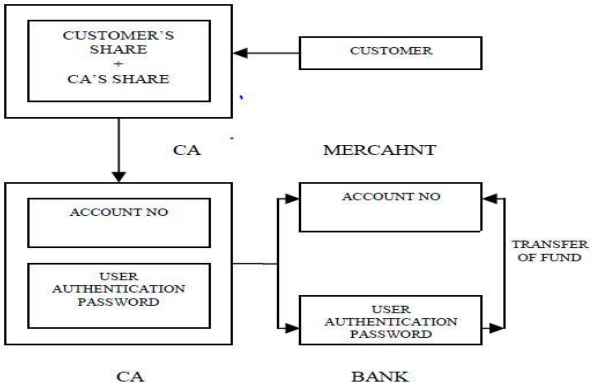
B. **Definition of Blocking Artifact Function**

During data hiding,each secret bit is embedded into one usable segment by modifying some of the appended bits.Thus the corresponding AC coefficients in the usable blocks are possibly modified, which, in most cases, may introduce blocking artifacts between a usable block and its neighboring blocks. Here we define the blocking artefact function which will be used in image extract and recovery[10].

VI METHOD EXTENSION

Customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method.Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form.A snapshot of two texts is taken and kept.One share is kept in the database of the certified Authority(CA) and the other share is kept by Customer.While shopping online, after selection of desired item and adding the item to the cart, preferred payment system of the merchant directs the customer to the portal of Certified Authority(CA).In the portal,customer submits his own share and merchant submits its own account details.Now the CA combines its own share with shopper's share and obtains the original image.From CA, merchant account details, cover text are sent to the bank.At the bank side,the customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA.After receiving customer authentication password, bank matches the customer authentication password with its database and after verifying genuine customer, transfers fund from the customer's account to the merchant's account. After the fund is recieved,the merchant's payment system validates receipt of payment using customer authentication information.The problem is that Certified Authority does not know to which bank to forward the cover text obtained by combining the two shares.But this can be overcome by appending nine digit routing or transit number of bank with customer authentication information.Presence of a fourth party, CA, ensures customer's satisfaction and security further as more number of parties are involved in the process. Cover text can be sent in the form of email from CA to bank to avoid rising suspicion.

Security Threat: During payment, merchant's payment system requires to direct the shopper to CA's portal but fraudulent merchant may direct shopper to a portal similar to CA's portal but of its own making and get hold of customer own share.

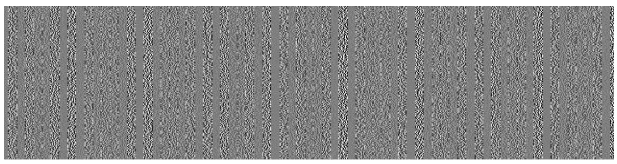


Snapshot account no and cover text

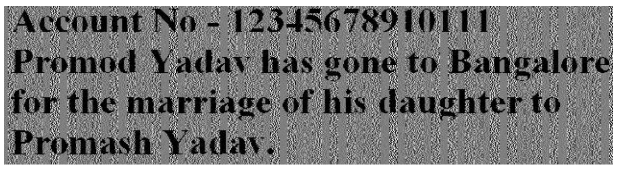
Account No - 12345678910111
Promod Yadav has gone to Bangalore for the marriage of his daughter to Promash Yadav.

Share 1 kept by customer.

Share 2 kept by CA



Overlapping of share 1 and share 2.



VII. CONCLUSION AND FUTURE WORKS

In this paper, a payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The payment system can also be extended to physical banking.Shares may contain customer photographic image or signature in addition to customer authentication password. In the bank, customer submits his own share and his physical signature is validated against the signature obtained by combining customer's share and CA's share along with validation of customer authentication password.This helps in preventing the misuse of stolen card and stops illegitimate customer.

VIII.REFERENCES

[1] Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang,
"Reversible Data Hiding in Encrypted JPEG Bitstream"," IEEE TRANSACTIONS ON MULTIMEDIA,vol. 16, no. 5,August 2014".

[2] Souvik Roy and P. Venkateswaran,"Online Payment System using Steganography and Visual Cryptography"," 2014 IEEE on Electrical, Electronics and Computer Science".

[3]K.Thamizhchelvy, 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, 2013.

[4]Juan Chen,Chuanxiong Guo,"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, 2010.

[5] Do Van Tuan, Tran Dang Hien,Pham Van At," *International Journal of Computer Science and Information Security",*Vol. 10, No. 8, August 2013.

[6] ShengDun Hu, KinTak U,"A Novel Video Steganography based on Non-uniform Rectangular Partition","IEEE International Transaction on Computational Science and Engineering CSE/I-SPA".

[7] Weiming Zhang, Biao Chen, and Nenghai Yu," Improving Various Reversible Data Hiding Schemes via Optimal Codes for Binary Covers",IEEE Transaction on Image Processing, Vol. 21, no. 6, June 2012.

[8] Xiaolong Li, Bin Yang, and Tieyong Zeng,"Efficient ReversibleWatermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection", IEEE Transaction on Image Processing, vol.20, no. 12,December 2011.

[9] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," Reversible Data Hiding", IEEE Transactions on Circuits and Systems for Video Technology, vol. 16,no. 3, March 2006.

[10] Diljith M. Thodi and Jeffrey J. Rodríguez,"Expansion Embedding Techniques for Reversible Watermarking", IEEE Transaction on Image Processing, vol.16, no.3, March 2007.