Combine Use of Steganography and Visual Cryptography for Online Payment System

V. Lokeswara Reddy, PhD
Associate Professor
Department of CSE
KSRM College of Engineering
Kadapa, YSR District. AP (INDIA)

T. Anusha
Post Graduation Student
Department of CSE
KSRM College of Engineering
Kadapa, YSR District. AP (INDIA)

ABSTRACT
A rapid growth in the E - Commerce market is seen in recent time in the whole extent of the world. With ever increasing popularity of online shopping, Debit/Credit card fraud and personal information security are major concerns for clients, Merchandiser and depository financial institution specifically in the case of CNP (Card Not Present). This paper presents a novel approach for providing limited information that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity stealing. This method uses combined application of Steganography and visual cryptography for this purpose.

Keywords
Steganography, InformationSecurity, Visual-Cryptograhy, Online-payment.

1. INTRODUCTION
Online shopping is the recovery of product data by way of the internet and go-forth of purchase club to completion of electronic purchase asking, sating of credit or debit card data/info conveyance of ware by mail order or home-delivery by courier. Persisting entity theft and phishing are the usual dangers of online-Shopping. Persisting entity thefts is the thievery of someone's persisting entity in the form of personal info/data for inducing purchase and used for wrong through that information for inducing purchase and spreading of bank accounts or setting Credit-Cards. Phishing is a malefactor mechanism that hires both social consumers/clients personal and individual data/info and financial account facts. Secure Social Layer (SSL) encryption forbids the taping of consumer information in transit between the consumer/client and the online merchandiser.

In this paper, a new method is proposed, that applies text based Steganography and visual cryptography, which derogates information dealing between consumer/client and online merchant but enable successful fund transfer from consumer's account.

1.1 Text based Steganography
In text Steganography, message can be hidden by shifting word and line, in open spaces, in word succession. Attributes of a conviction such as number of phrases, number of characters, num of vowels, location of vowels in a word are also used to hide private message. The advantage of choosing text Steganography over other Steganography techniques is its smaller memory requirement and simpler communication.

1.2 Visual Cryptography
Visual Cryptography (VC), proposed by Naor, is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication groove. Only blending the k shares or more give the original secret image.

2. PROPOSED SYSTEM
In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is attained by the unveiling of a central Certified Authority (CA) and combined application of Steganography and visual cryptography. The information obtained by the merchant can be in the form of account number related to the card used for shopping. The information will only formalize receipt of payment from authentic customer. fig 1 shows proposed payment system.

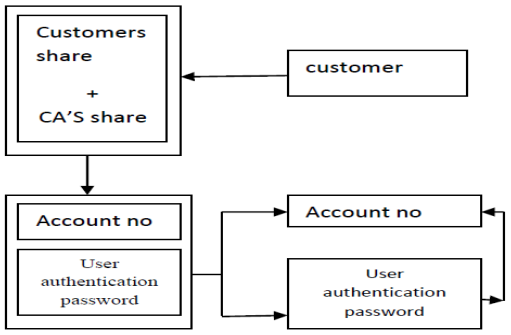


Fig 1: proposed payment method

2.1 Advantage
1. Proposed method minimizes customer information sent TRANSFER OF FUND to the online merchant.

2. So in case of a breach in merchant's database, customer doesn't get involved.

3. It also forbids unlawful use of customer information at merchant's side.

4. Presence of a fourth party, CA, enhances customer's atonement and security further as number of parties are involved in the process.

5. Usage of Steganography ensures that the CA does not know the customer authentication password thus maintaining customer privacy.

6. Cover text can be sent in the form of email from CA to bank to avoid rising suspicion. Since customer data is circulated over 3 parties, a breach in single database can easily be contented.

3. RELATED WORK

A short measurement of related work in the area of banking security based on online shopping by combine use of Steganography and visual cryptography proposes this methods to eradicate the frauds through text based Steganography hiding data rather than using properties of sentences and each letter is assigned to a num in the range of (0-15) Number assigned in range (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is any integer from 0 to 11.

Table 1:Number assignment

Letter	Number assigned	Letter	Number assigned
E	15	M	7
A	14	H	7
R	13	G	6
I	13	B	5
O	12	F	4
T	11	Y	4
N	11	W	3
S	10	K	3
L	10	V	3
C	9	X	2
U	8	Z	2
D	8	J	1
P	7	Q	0

The above table 1 shows the number assigned to a letter.

3.1 Encoding

In this process, Steganography uses characteristics of English language such as inflexion, fixed word order and use of circumlation for hiding data rather than using properties of a conviction. This gives manipulable and freedom from the point view of sentence construction but it increases computational complexity.

3.1.1 Text encoding process

Input: Text file

Output: secret key image shares

Step 1: Representation of each letter in secret message by its equivalent ASCII code.

Step 2: Convert ASCII code into equivalent 8 bit binary number.

Step 3: Divide 8 bit binary number into two 4 bit parts.

Step 3.1.1: Choose the desirable letters from table 1 corresponding to the 4 bit parts.

Step 3.1.2: Meaningful sentence construction by using letters obtained as the first letters of suitable words.

Step 4: Converted sentence can be generated as secret key image.

Step 5: Secret key image can be divide two portions/shares are obtained in jpg form.

3.2. Transaction in online shopping:

In this module traditional online shopping consumer selects items from online shopping portal and then is directed to the defrayal foliate. Online merchandiser may have its own payment arrangement or can take action of third party payment systems such as Pay-Pal, pay-online-system, WebMoney and others. In the claiming portal node/user submit his or her credit or debit card details such as credit or debit card numerals, mention on the card, termination date of the card.

3.2.1 Customer Authentication:

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 master form. Now a informal photograph of two texts is taken. From the informal photograph image, two portions/plowshares are generated using visual cryptanalysis. Now one portion/plowshare is kept by the customer and the other portion/plowshare is kept in the database of the certified authority.

3.2.2 Certification Authority Access

During shopping online, after selection of desired item and adding it to the go-cart, opted defrayal system of the merchandiser directs the customer/node to the Certified Authority imposing entarnce. In the imposing entrance, shopper accedes its own portion/plowshare and merchandiser takes its own record details. Now the CA unites its own portion/plowshare with shopper's plowshare and obtains the master image. From CA now, merchandiser record details, screen text are sent to the bank where customer authentication password is recovered from the cover text.

3.3. Decoding

Paces for decoding:

Input: Two secret key images/shares

Output: Original secret key image

Step 1: First letter in each word of cover message is taken and represented by corresponding 4 bit number.

Step 2: 4 bit binary numbers of combined to obtain 8 bit number.

Step 3: ASCII codes are obtained from 8 bit numbers.

Step 4: Finally, secret message is recovered from ASCII codes.

Step 5: Secret key image can be restored.

Customer authentication information is sent to the merchant by CA. Upon obtaining client/node authentication phrase known only to a restricted group, bank matches it with its posses records and after sustaining authorized client/node, transmits fund from the client/node record to the stated merchandiser account.

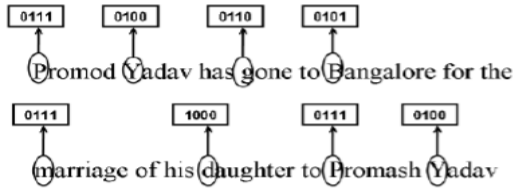


Fig 2:cover image

3.4 Method extension

The payment system can also be extended to physical banking. Shares may contain customer image or signature in addition to customer/client certification password. In the bank, customer submits its own share and customer physical signature is validated against the signature obtained by combining customer's share and CA's share along with validation of customer certification password. It forbids pervert of stolen.

4. EXPERIMENTAL WORK

When the scheme is executed the GUI(Graphically based User Interface) is displayed. The snapshot of the main window is shown in below figure 3.It shows the bank registration for secret key generation.

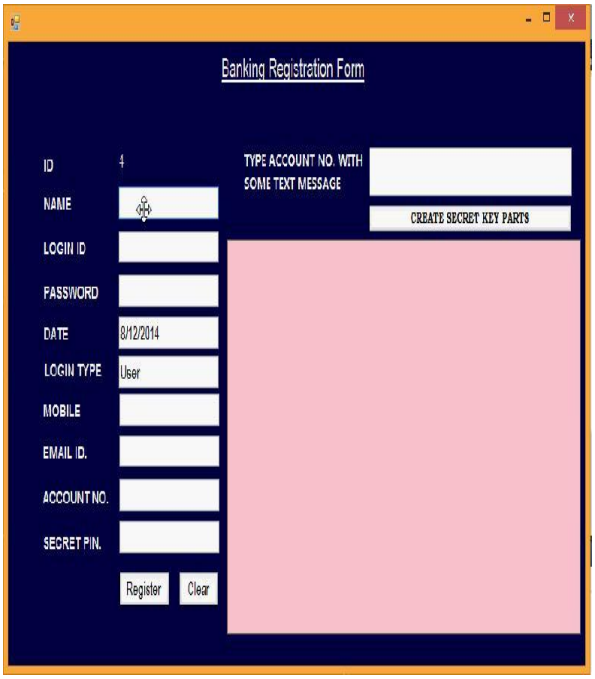


Fig 3: Bank registration form

By the above snapshot banking registration the below window can be displayed with secret key generation and that secret key can be divided into two shareswhich was shown in the below fig 4.It generates the secret key images.

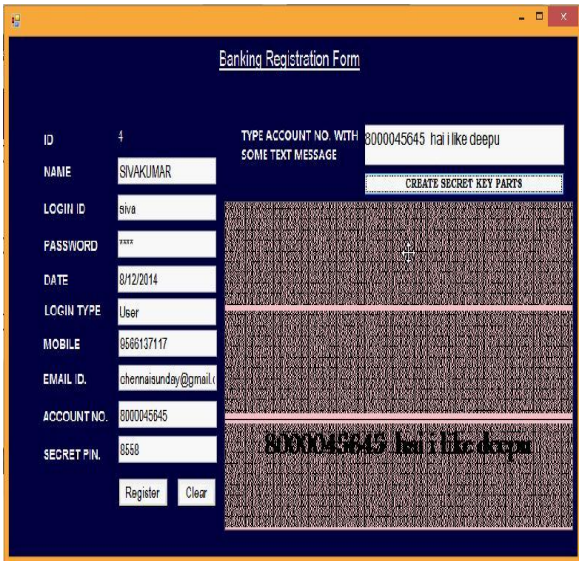


Fig 4: secret key generation

The secrete key obtained is utilized in the online transaction for secure transmission.Below fig 5 shows in the transaction one secret key image is inserted by the client/customer, the other is inserted by the certified author which was stored in the bank while registration.

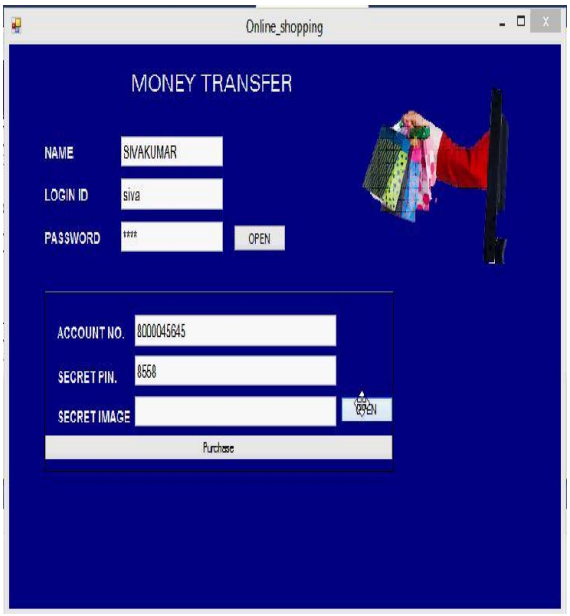
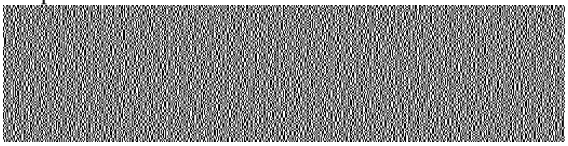


Fig 5: money transfer in online shopping

The proposed method applied on different key images with its results is shown below.

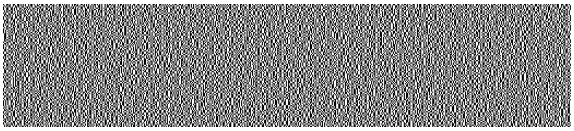
Case 1: key extraction for client l

1. Transaction of client/customer named and transaction is completed.



Secret key image 1

+

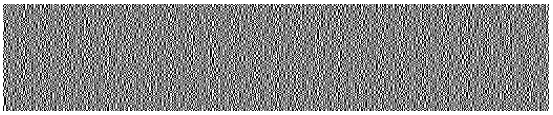


Secret key image 2

=

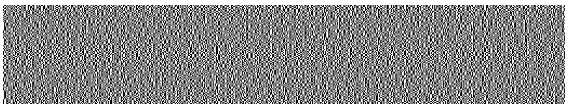
Shows when transaction complete.

2. Transaction of customer/client named anu when transaction not completed.



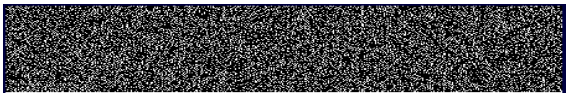
Secret key image 1

+



Secret key image 2

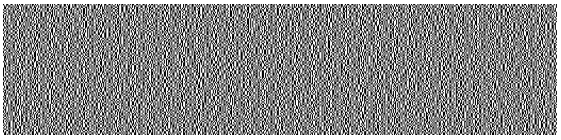
=



Shows when transaction not completed.

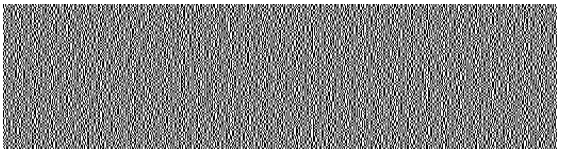
Case 2: Key extraction for client 2

1. Transaction of client/customer named sai and transaction is successful.



Secret key image 1

+

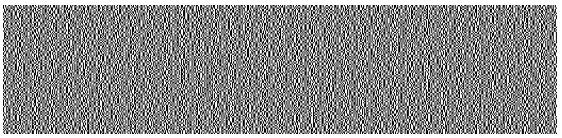


Secret key image 2

=

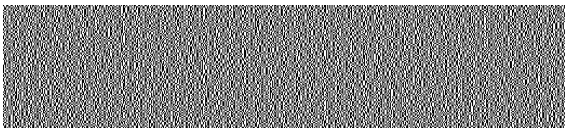
Shows when transaction is completed

2. Transaction of customer/client named sai and transaction not completed



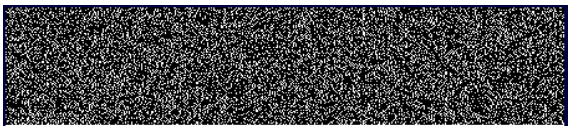
Secret key image1

+



Secret key image 2

=



Shows when transaction not completed.

5. CONCLUSION

In this paper, we propsed a payment system for online shopping by combining text based Steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchandiser's side. The computing is implicating only with prevention of identity theft and customer data security. In likening to other banking application which uses Steganography and visual cryptography are basically applied for the physical banking, the proposed method can be applied for the E-Commerce with focus area on payment during online shopping as well as physical banking.

6. REFERENCES

[1] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shoppingOnline," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011. Javelin Strategy & Research, "2013 Identify FraudReport, https://www.javelinstrategy.com/brochure/276.

[2] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol.35, Nos. 3 & 4, pp. 313-336, 1996.

[3] M. Naor nd A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[4] **4.**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.

[5] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies.

[6] C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology.

[7] A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler,H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services on demand: Wsla-driven automated management,"IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.

[8] M. Wang and T. Suda, "The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications," in Proc. of the IEEE Symposium on Applications and the Internet.

[9] N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems.

7. AUTHOR PROFILE

Dr. V. Lokeswara Reddy did his Ph. D in Computer Science and Engineering from JNTUA, Ananthapuramu in the year 2015. He did his M. Tech (CSE) from SRM University, Chennai in the year 2005. He did his M.C.A from S.V. University, Tirupati in the year 2000. He has a total of 13 years of experience in teaching. Currently he is working as Associate Professor at K.S.R.M College of Engineering, Kadapa. He has presented 9 papers in International, National Conferences and published 13 papers in International journals.

T.Anusha did her B.Tech (CSE) from JNTUA, Anantapuramu in the year 2013. She is pursuing her M.Tech (CSE) from JNTUA Anantapuramu, Andrapradesh. She is currently doing her M.Tech in K.S.R.M College of Engineering, Kadapa.