www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-7, Issue-2, March-April 2017

International Journal of Engineering and Management Research

Page Number: 593-598

A Bird Eye View on Secure Banking by using Different Image Based Hiding Technique Encryption and Decryption

Garima Gupta[1], Prof. Sumit Dhariwal[2]

[1]Research scholar, Sager Institute of Research and Technology – Excellence, Bhopal, RGPV, INDIA

[2]Computer Science Engineering Department Sager Institute of Research and Technology – Excellence, Bhopal, RGPV, INDIA

ABSTRACT

In the present scenario of information Technology, use of Internet is becoming quite popular for accessing information on any topic of our interest. Internet banking is the term used for new age banking system. Internet banking is also called as online banking and it is an outgrowth of PC banking. Internet banking provides a change from the traditional way of face-to-face contact at a bank's counter during office hours to a remote way by online network connection anywhere at any time. Time to time increases the use of E-banking number of cybercrime also increases. To avoid such type of problem researcher introduced new techniques for secure data communication. In such a manner image based data hiding is one of them. In this work we discuss the different data hiding techniques in image. This survey paper shows summery on different data hiding techniques. Data hiding in the image is art or science in which embedding the secret data into the image using different methods like image stenography, cryptography and visual cryptography. Also discuss the quality check parameters like SSIM, visual quality of the images in terms of edges and others human perception.

Keywords-- E-banking, Steganography, cryptography, Structural similarity index measurement (SSIM) and Image data hiding

I. INTRODUCTION

In the present age of information Technology, use of Internet is becoming quite popular for accessing information on any area of your interest. It also provides tremendous opportunities to, researchers and professionals for getting information on matters related to academic and professional topics and lot more. In the present world, most of the people who have computers around themselves use Internet to access information from the World Wide Web, exchange messages & documents and e-services.

Internet banking is an alternative banking channel. It offers a change from the traditional way of standing in the waiting area in front of a bank's counter during office hours to an automatic way through online network connection, anywhere, at any time, around the world. Internet banking provides many benefits not only for a bank's customers but also for a bank itself as well. The benefits the users gain include convenience and flexibility. Users also enjoy a self-service, reduced stress of standing in line in front of bank employees, and reduction in transaction cost. [17]

II. SECURITY ISSUES IN SECURE BANKING

Security is the main issue for both online banking and E banking. There are different type of attacks occur in the Net banking and E-banking.

Phishing*:* Phishing is a kind of scam where the scammers masquerade as a trustworthy source in attempt to gain private data such as PINs, and credit card details etc. through the internet.

Malware: Malware, mainly spyware, is malicious software camouflaged as legitimate software planned to accumulate and transmit private data, such as PINs, without the customer's consent or knowledge.

Identity theft: Identity theft is a crime in which a fraudster obtains key pieces of personal data, such as bank information, date of birth or driver's license numbers, in order to impersonate somebody.

Trojan horse/Trojan: Trojan horse are the most dangerous type of attack in which attacker can directly gain unauthorized access to victims systems.

Virus: Virus is a computer program that designed to replicate itself from one computer to another.

There are major attacks occurs in online banking and E-banking.

III. SECURE SOLUTION

There are different data hiding methods and techniques are available, these techniques are used secure on line banking and E banking for secret data and secret communication in public channel like steganography, cryptography and others.

Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, data integrity, and of data authentication. In cryptography a plain message is encrypted into cipher text and that might look like a meaningless jumble of character whereas in case of steganography, the plain message is hidden inside a medium that looks quite normal and does not provide any reason for suspecting the existence of a hidden message. Such an image is called as stego-image. Data hiding conceals the existence of secret information while cryptography protects the content of messages. More and more attention is paid to reversible data hiding in encrypted images.

1. *Reversible data hiding*

Reversible data hiding can be defined as an approach where the data is hidden in the host media that may be a cover image. A reversible data hiding is an algorithm, which can recover the original image loss less after the data have been extracted.

The transmitter side of such systems involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be hidden and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data. The reversibility means that not only the embedded secret data but also the encrypted cover image must be extracted lossless at the receiver side

2. *Background*

Image data hiding processes are essential part for any secret data communication. When hide the secret data in an image quality of image degrade. Hence techniques that asks for to enhance the interpretability or perception of images for the human viewers and providing higher input for the automated image process techniques. In this paper focused on different data hiding techniques.

3. *Visual Cryptography*

Visual Cryptography is an emerging crypto-graphic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human visual system, without the aid of computers. It uses a simple algorithm unlike the complex.

It needs neither cryptography knowledge nor complex computation. Visual cryptography technique (for black and white images) is introduced by Naor and Shamir in 1994 during EUROCRYPT'94.

For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are random dots without revealing the secret information. Basic visual cryptography is expansion of pixels. Visual cryptography is a method of sharing a secret image among a group of participants, where certain group of participants is called as qualified group who may combine their shares of the image to obtain the original, and certain other group is defined as forbidden group who cannot obtain any information on the secret image, even if they combine knowledge about their parts. The scheme gives an easy and fast decryption process that is done by stacking the shares onto transparencies to reveal the shared image for visual inspection.

4. *Steganography*

Image steganography terminologies are as follows:-

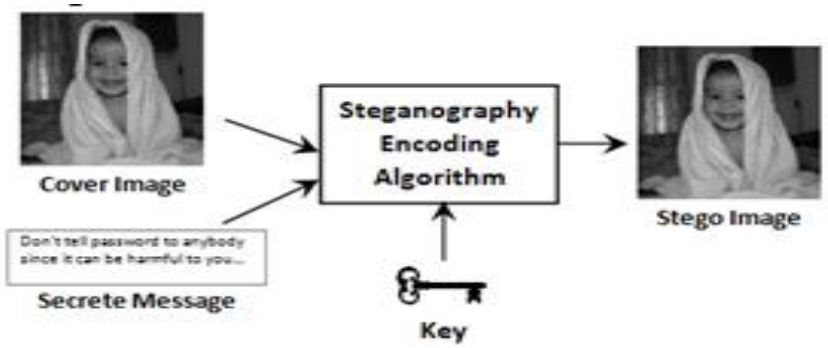
Cover-Image: Original image which is used as a carrier for hidden information.

Message: Actual information which is used to hide into images. Message could be a plain text or some other image.

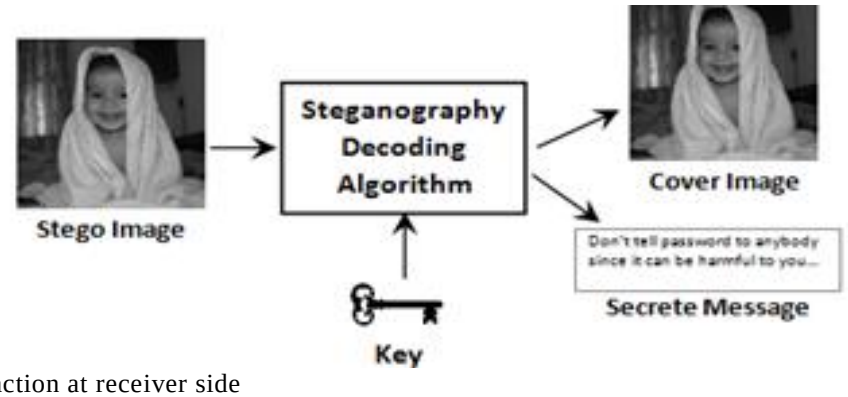
Stego-Image: After embedding message into cover image is known as stego-image.

Stego-Key: A key is used for embedding or extracting the messages from cover-images and stego-images.

ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962



(a) Stego Image Generated at Sender Side



(b) Message extraction at receiver side

Fig.1. Concept of Steganography

Generally image steganography is method of information hiding into cover-image and generates a stego-image. This stego-image then sent to the other party by known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [ ]. Basic diagram of image steganography is shown in Figure 2 without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm un-hides the message from stego-image.

IV. IMAGE BASED SECURE ONLINE AND E- BANKING

During this in survey discuss couple of new concepts algorithms of the data hiding with the help of visual cryptography.

A. *Steganography and Visual Cryptography for Online Payment System (2015).*

This research presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. 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 channel. Only combining the k shares or more give the original secret image. Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing [1].

B. *Online Payment System using Steganography and Visual Cryptography (2014)*

A rapid growth in E-Commerce market is seen in recent time throughout the world. With ever

increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose [3].

C. *B. Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding information in Text (2013).*

Steganography (A rough Greek translation of the term steganography is secret writing) has been utilized in various forms for 2500 Years. It's found use in variously in military, diplomatic, personal and intellectual property applications. Concisely declared, steganography is the term applied to any variety of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. This work can explore steganography from its earliest instances through potential future application steganography, in its multitude of forms, has been in use virtually for thousands of year. It would appear that based on the variety of forms that steganography messages can take that there could be steganography content on the internet. Location of some varieties of steganography content would requires techniques apart from statistical identification not the least of that can be visual examination notwithstanding the ability to encrypt. Whereas practical uses of steganography, with the exception of watermarking, appears to be comparatively limited with the abundance of alternative techniques freely available, it will possible fill a distinct segment for some activities. Consider that activity an object in plain sight, recall Edgar Allen Poe's "The taken Letter", can on occasion be the most effective possibility. [4].

D. *New Visual Steganography Scheme for Secure Banking Application (2012).*

Core banking is a set of services provided by a goggle of networked bank branches. Bank customers may access their funds and perform different straight forward transactions from any of the member branch offices.

The most important issue in core banking is the credibility of the customer. Attributable to inescapable hacking of the databases on the web, it is continuously quite difficult to trust the information on the internet. To solve this problem of authentication, are proposing an algorithmic program based on image processing, improved steganography and visual cryptography. This paper proposes technique of encrypt the secret of a customer by improved steganography, most of the steganography techniques use either three or four adjacent pixels around a target pixel whereas the proposed technique is in a position to utilize at most all eight adjacent neighbors So that imperceptibility price grows bigger and then dividing it into shares. Total number of shares to be created is counting on the scheme chosen by the bank. When two packages created, one is stored in the bank information and also the others kept by the customer. The customer needs to present the share during all of his transactions. This share is stacked with the primary share to get the original image. [5]

V. PROPOSAL FOR ENHANCED SECURE E BANKING

The structure of proposed method is broadly divide into the two parts. Transmitter end and receiver end. The flow charts of both end is also described in this chapter. First describe the transmitter end. The transmitter end is based on the encoder part. In this end generate the information and also create the cover image (CI) and postern image (PI).

Transmitter end (Encoder Part)

The transmitter end is the important part of the proposed method. In the transmitter end is also known as an encoder part of the proposed method. In this part create the stego image (SI). Stego image is the summation of secret data and hiding object that is cover image (CI). In this part there are three important terms used here.

- Cover image (CI)
- Secret Data (SD)
- Postern image (PI)

Cover image (CI)

Cover image is the image in which secret data (SD) is hide. In the proposed work focused on spatial domain. It means that secret (SD) data is hide into the only in pixels. There are different type of cover image data sets are available in the field of image processing. In the proposed method used a standard data set images.

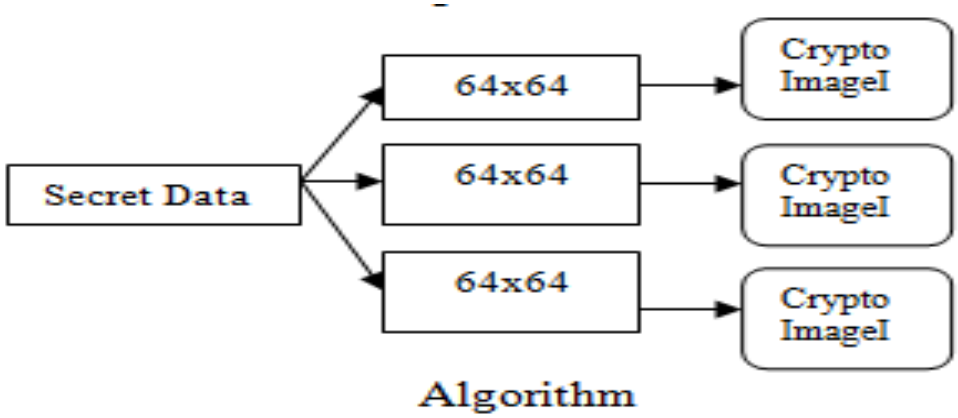
Secret Data (SD)

Secret data is the data in which is hide into the cover image. The quality of proposed work is based on the secret data. Secret data is generated at the user end and embedded into the cover image. Similar that secret data is obtain at the receiver end by postern image (PI). There are different type of secret data probable based on user end. In general secret data is in binary form, images and also ASCII based data available.

For the embedding of secret data first apply cryptography add secret data into 64X64 small image and create 3 stego image with the least significance bit.

1. 64x64 add personal details
2. 64X64 add Account Details

3. 64X64 add one time password



Postern Image (PI)

Postern image is created or generated when embedded the secret data into a cover image. The output if the summation of cover image and secret data is known as a stego image (SI).

Stego image is generated at the transmitter end (Tx) and flow in the communication channel (Internet world) like wide area network. This stego image is received at the receiver end (Rx). After the receiving of stego image apply the encoding process and obtain the secret information.

Vice versa process apply in the receiver end.

VI. CONCLUSION

In this survey paper present an over view online banking profit and losses. Also discuss the current generation faces the online problems of different attacks in the E banking and online banking. Discus the different data hiding process of images that is used in the online and E banking systems. In this survey discuss about data hiding and also reversible data hiding schemes. A short discuss on steganography, cryptography and visual cryptography. At the last discuss the proposal for secure data communication for E banking and Net banking using proposed algorithm. In the future work we will implement this proposed method on Maltab and enhance the result.

REFERENCES

[1] S.Adhikesavan and N.Sathish , "Stegano graphy and Visual Cryptography for Online Payment System" , International Journal of Scientific Research Engineering & Technology, pp. 153-1603, March 2015.

[2] Ms. Neha shrivastava and Prof. Mr. Toran verma, "A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency", International Journal Of Advanced Research In Computer Engineering & Technology, pp.-1005-1009, March 2015.

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

[4] K. Bennet, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Ceria Tech Report, 2013.

[5] S.Premkumar and A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application," Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumara coil, India, 2012.

[6] K. Thamizhchelvy and 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, 2012.

[7] ShengDun Hu and KinTak U, "A Novel Video Steganography based on Non-uniform Rectangular Partition", 14th IEEE International Conference on Computational Science and Engineering, pp. 57-61, 2011 IEEE.

[8] Jaya, Siddharth Malik, Abhinav Aggarwal And Anjali Sardana, "Novel Authentication System Using Visual Cryptography", pp. 1181-1186, 2011 IEEE

[9] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.

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

[11] KalavathiAlla, Dr. R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography," Proceeding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.
[12] ChetanaHegde, S. Manu, P. DeepaShenoy, 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, pp. 65-72, Chennai, India, 2008.
[13] Juan Chen, ChuanxiongGuo, "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, 2006.
[14] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.
[15] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.
[16] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
[17] http://eprints.utm.my/38968/3/AliSalehAliAl-AjamPFPPSM2013CHAP1.pdf.