IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Information Security Using Steganography: A Review

Monika

M.Tech (CSE), BPS Mahila Vishvavidyalya, Khanpur Kalan, Sonipat, India

*Corresponding Author: malikmonika315@gmail.com,

Available online at: www.ijcseonline.org

Accepted: 13/Aug/2018, Published: 31/Aug/2018

***Abstract*—** In modern era of communication there is lot of information exchange and every one need more and more secure communication. In order to provide secure communication stenography is widely used. The present paper provides conceptual framework on stenography that became basis for secure communication. Stenography is process of hiding secret information in any other message and provide secures communications. It consists of cover, hiding process, and un-hiding process along with channel on sender and receiver side. Stenography is implemented with the use of secret data in files. In first phase concept of stenography has been discussed & represents definition of stenography, working of stenography respectively. Existing research and benefits of stenography have been discussed in second phase respectively. Discussion has been made on designing techniques of stenography in order to enhance security. Next phase is considering challenges to existing researches have been explored in this paper. Such analysis would be beneficial to consider better enhancement in existing security mechanism. As there would be more probability of advance research if limitations of existing work is considered. At end of research in Last phase scope of research has been discussed.

***Keywords*—** Steganography, Encryption, Decryption, Encoder, Decoder

I. INTRODUCTION

Steganography is process of hiding of a secret message within an ordinary message [1]. Anyone scanning information would fail to know if it is containing encrypted data. Steganography may be considered as an art, science, or practice. Some messages, graphics, or files works as a cover for few other messages, graphics, or files [2]. Concept of steganography is not the unknown concept. This concept is associated with digital world. Many experiments have shown that there are various ways to hide the information inside many types of digital files.

As we talk about today's digital steganography, usual means are used for the encryption of the information. After this a special algorithm is used for insertion. It uses the information which is the part of a special file format. The JPEG image form is used to show its format. Same coloured pixels are shown by all bits which are repeated continuously. The information that is encrypted is easy to apply to this required information randomly. The output would be the non-encrypted data in which there are regular "noise" patterns of information.

STEGANOGRAPHY

Technology has enabled embedding of hidden messages efficiently and easily in modern computer age. The message is encoded by computerized tools. It is hidden in another file. It is defined by Johnson that steganography is an art of concealing whether information is present or not. Its goal is to cover up the fact that message should be existed in first place (Anderson and Petit colas, 1998). In 1996, the terminology in steganography described as follows was defined by Information Hiding Workshop in Cambridge (Pfitzmann, 1996). The implanted information should be hidden in cover or original. It can also be hidden into innocent file such as an image, audio, the text, or video. The process is known as embedding, and embedded data collect form Stego data [3].

WORKING OF STEGANOGRAPHY

Steganography works on secret data. It does so by increasing secret bits in files. These are photos or audio files etc.

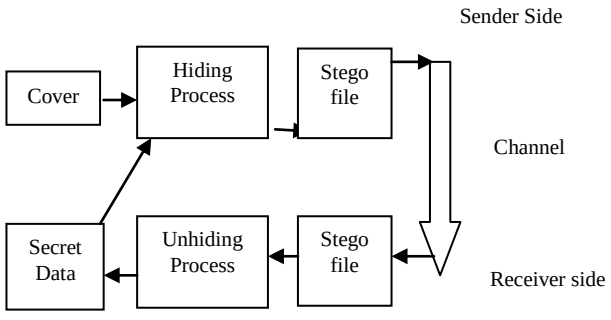

Fig: 1 Working of Steganography [4]

It is got more appealing due to the reality that this not used extensively. Secondly it is very difficult to crack. [5]. It is the best method to send information which is highly sensitive

whether personal or business. This information can be sent by using internet sources like e-mail on Web, or by social channels as Twitter or Face book [6].

Two types of popular approaches are discussed here:
The Hidden information which have information or information in any other form as in file type or, in form of JPG images, resolution & colour depth of photo. It may be developed in the file header [7].

If it is desired that whole file should not be damaged or altered, only those parts of the information should be altered which are not important to total file. Now the working has been discussed. Each byte is constructed of 8 bits [8]. If the image pixels are red or white, defining all of the 8 bits is not important [9]. It is very perfect spot for hiding secret data because a) it doesn't increase size of the file & b) it doesn't change the file. One of is to Embedding a text file in an image file is the most prevailing steganographic technique. Any person who is observing image file will find no difference between original file and embedded file. Storing of messages are done by using those bits in the information file which are least important. The main challenges to enterprises must be clear. These are based on abilities of steganography. Clearly a generic image file can be attached by an employee through email. This image may have an embedded. This document can be full of company secrets with its code.

Rest of the paper is organized as follows, Section I contains the introduction of Information Security using Stegnography, Section II contain the Existing Research, Section III contain the Benefits of Existing Researches, Section IV contain the Challenges to Existing Researches, Section V explain the Legal Issues and challenges, Section VI describes Future Scope.

II. EXISTING RESEARCH

The previous research is described in this section. However, there are lot of researches in field of steganography but many of them has been mentioned here.

G. Abboud et al. (2010) had make study on Steganography & Visual Cryptography in Computer Forensics [3] in which they have explained some definitions of steganography. Visual cryptography is elaborated with many studies. These studies are done on different algorithms of each type.

Sana Shiva et al. (2015) made research on Secure E-marketing Using Steganography & Emergence of Cryptography [2] in this work was elaborating a technique. This technique is used for securing personal information from fraud which may be leaked out in Online Shopping. The main reason to adopt E-commerce is any password which is identified from any attack and affects a customer or merchant.

S. R. Navale1 et al. (2015) proposed that Online transactions can be secured by using Text Steganography & Visual Cryptography. [3] Under it the information of consumer's payment is minimized because it is needed for fund transferring.

Pradnya S. Nagdive et al. (2015) proposed the Visual Cryptography & Steganography. [4] Here privacy is maintained. The certainty of pictures may be a spirited space for analysis. Here two totally different approaches are followed. The first is encrypting pictures by encoding algorithms with the use of keys.

Priyanka More et al. (2016) explained about online Payment System. The Payment System can be used through Steganography & Visual Cryptography [5]. According to this research, major issues of concern for customers during online shopping that there may be many frauds in debit card or credit card. Hence security of personal information is also affected.

III. BENEFITS OF EXISTING RESEARCHES

In Steganography & Visual Cryptography in Computer Forensics [10] researchers studied that use of algorithm in a solid reconstruction method permits the researchers for reconstructing shares back in the unaltered, original image [11]. This algorithm has been designed to present a vast area. Further investigation can be done by using this algorithm. With a keen use of this algorithm several recent venues would be opened in the world of forensics & anti-forensics [12]. Information about many issues can be obtained from it. The cryptography [13] is with perfect reconstruction to the image in hidden data.

In Secure E-marketing Using Steganography & Emergence of Cryptography author is providing a how a security can be provided under Online Shopping [14]. This technique would protect personal information from fraud. Potentially E-commerce is admitted by a password. It may track any attack which may affect customer or merchant. This algorithm permits concerns of major security for personal information which are debit or credit details in the absence of the card.

Here an online payment system is represented Visual Cryptography & Text Steganography which is much secured. This system provides the availability to do payments to the online merchant or online supplier. The channel between consumers & payment processors is used as a payment portal. It uses many security tools to provide security to a consumer's payment information when an online transaction is done. [15].

As there is continuous growth in E-Commerce market, it has become necessary in new time to use Digital wallet or online System [16]. Many concerns for customers in the online shopping are debit card or credit card frauds. Theft of Identity & phishing are the common challenges of online shopping.

IV. CHALLENGES TO EXISTING RESEARCHES

However existing researches are providing security to data. But they have certain limitations. Some of them are takes lot of time to provide protection to data. Some of researches are platform dependent thus they are not application of every hardware & software platform. Several researches are providing limited security in case of e-commerce applications [17].

V. LEGAL ISSUES AND CHALLENGES

Many laws who have technology are very difficult to enact. These are also very difficult to enforce in the age of Internet. Here an issue of jurisdiction may be arise due to crossing international borders and cross state lines. It may be that an issue is illegal in one jurisdiction but legal in another. It includes a provision that is wire fraud. It was extended to encompass Internet later. If any part of the telecommunications system is used, it is a criminal act and now a federal offense.

Privacy vs. Security

The position of ACLU's is on privacy and technology. The main issue is that United States is at the risk of getting a surveillance society. Two consecutive developments make the basis for this tremendous explosion. It is providing surveillance-enabling technologies. The vision of 'Big Brother' given by George Orwell' has now become possible technologically. As the technological observation is developing between us, the legal restraints keep it by trampling our privacy.

International Travel

In the end, it may be said that steganography is not illegal. Here possession may be the cause for alarm in various parts of world. There are many international travellers. These include business travellers. Some coded messages are unbreakable. These messages are not hidden. Suspicion may be risen by it. There may be some countries where encryption is illegal. In case of finding hidden digital messages, there would be trouble for the owner of equipment. Utilization of steganography should need to be considered carefully.

VI. FUTURE SCOPE

In Steganography & Visual Cryptography methods shows recent way of implant information particularly in Multiresolution analysis, there are different ways of getting Multiresolution; this thesis has made use of Multiresolution analysis on wavelets & Curve lets [18]. Experimental analysis has proved that Curve lets is best Multiresolution transformation available.

This is to make secrete communication, in addition to this crypto way of embedding gives us higher end of security. Even if person gets both stego & cove image he needs key to retrieve data, without key one can't recover information [19]. Thus additional security is incorporated to normal Steganography technique [20].

REFERENCES

[1] George Abboud (2010) Steganography & Visual Cryptography in Computer Forensics 2010 Fifth International Workshop.

[2] Sana Shiva et al (2015) Secure E-marketing Using Steganography & Emergence of Cryptography Journal of Computer Science & Information Technology IJCSMC, Vol. 4, Issue. 1, January 2015, pg.532 – 538

[3] S. R. Navale1 (2015) Approach in case of Secure Online transaction using Visual Cryptography & Text Steganography, IJERT Vol. 4 Issue 03, March-2015

[4] Pradnya S. Nagdive (2015) Visual Cryptography & Steganography: A Review IJARCS & Management Studies Vol 3, Issue 1, January 2015

[5] Priyanka More, et al. (2016) Online Payment System using Steganography & Visual Cryptography, International Journal of Computer Engineering In Research Trends, Volume 3, Issue 4, April-2016, pp. 157-161

[6] Souvik Roy et al., Online System to make Payment with the help of Steganography & Visual Cryptography, IEEE Conference on Electrical, Electronics & Computer Science, Jadavpur University, Kolkata, India. 2014.

[7] Thiyagarajan, et al. "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE-International Conference on Communications & Computational Intelligence, 2010.

[8] N. Chou, et al. ,Client-side defense against web-based identity theft,' in Proc. 11th Annu. Netw. Distribut. Syst. Secure. Symp, San Diego, CA, Feb. 2005.

[9] Anthony Y. Fu, Liu Wenyin, "Detection of Phishing Web Pages with Visual Similarity Assessment Based on EMD",IEEE Transactions on Dependable & Secure Computing, v 3,n 4, October/December 2006.

[10] S. Roy, P. Venkateswaran, "Online System to make Payment with the help of Steganography & Visual Cryptography", IEEE Conference on Electrical, Electronics & Computer Science, vol. 6, no. 2, pp. 88-93, 2014

[11] M. Suresh, B. Domathoti, N. Putta, "Online Secure E-Pay Fraud Detection in E-Commerce System Using Visual Cryptographic Methods", International Journal of Innovative Research in Computer & Communication Engineering ,vol. 3, no. 8, pp. 7519-7525, August 2015.

[12] Rahna E, V. Govindan, "A Novel approach to protech, Lossless Steganography using Unlimited Payload & Without Exchange Of Stegoimage", International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp. 1263-1270, July 2013.

[13] R. C. Gonzalez & R. E. Woods," Digital Image Processing" Upper Saddle River, NJ: Prentice-Hall, 2006.

[14] [14] C. Chan, L, et al., "Data hinding in images with the help of LSB substitution Recognition of Pattern", pp. 469– 474, August 2004.

[15] N. Shrivastava1 et al., "Survey on various mechanisms to make Image Steganography with enhanced Efficiency", IJARC Engineering & Technology , vol. 4, no. 3, pp. 1005-1009, March 2015

[16] M. Kutter, S. Winkler, "A Vision-Based Masking Model for Spread-Spectrum Image Watermarking", In proceedings International Conference on Computing, Electronics & Electrical Technologies, pp. 313-336, 2004.

[17] X. Li, et al., "A Generalization of Matching in case of LSB", IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, February 2009.

[18] P. Vaman, C. Manjunath, Sandeep , "Integration of Steganography & Visual Cryptography for Authenticity", International Journal of Emerging Technology & Advanced Engineering, vol. 3, no. 6, pp. 80-84, June 2013

[19] C. Hegde , et al. , "Secure Authentication using Image/graphical Processing along with Visual Cryptography for Banking

Applications", in Conference of Advanced Computing & Communications, pp. 65-72,2013

[20] A. Suklabaidy a, et al., "Visual Cryptographic Applications", International Journal on Computer Science & Engineering, vol. 5, no. 06, pp 455-464, June 2013.

Authors Profile

Monika is pursuing M.Tech (Computer Science and Engineering) from Bhagat Phool Singh Mahila Vishavidhyalya (BPSMV), Khanpur Kalan, Sonipat. She has completed her B.Tech (Computer Science and Engineering) in 2016 and Polytechnic in 2013 from Bhagat Phool Singh Mahila Vishavidhyalya (BPSMV), Khanpur Kalan, Sonipat, India.

