IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Current Trends In Steganography

Kirti [1], Parmod Sarowa[2]

[1]Computer Science Engg., Assistant Professor, MSIET, M.D.U., India, Haryana , Rohtak
[2]Electrical Engg., Assistant Professor, MSIET, M.D.U., India, Haryana, Rohtak

Available online at: www.ijcseonline.org

Accepted: 14/Jul/2018, Published: 31/Jul/2018

***Abstract*-**Steganography relies on volatility in order to perform information hiding inside apparently innocuous payloads. Steganography helps in create secure communication between two parties, without any mediator noticing the presence of the particular communication. Steganalysis is the parallel to steganography. A steganalyst tries to find out the presence of a covert communication between two parties and either modify their communication.
Many different techniques are introduced to make communication more secure by using steganography. All of them are proven to be secure in there own way. Many new techniques are coming in existence from past few years. In this paper, we review the different techniques that has already introduced.

***Keywords*-** Steganography, QR code, DWT, Bluetooth, Logistic Map , DNA.

I. INTRODUCTION

In recent years, with the expansion of internet and communication technology, the data transfer is very easy, handy, speedy and correct. Since internet provide open and public communication which is convenient but risky and peril[1,7]. Data security is more important and become an interest of era for mostly researchers . Image is eminent for the unique features such as immense data, low competence and high link among pixels.

In this paper we review new technologies that are using steganography for the sake of society and can be used in various fields . As we know
that steganography is a data hiding and data security technique. Some of them are:-

- Image steganography and data hiding in QR codes Image steganography for criminal cases.
- A Novel method for Bluetooth Pairing using Steganography
- A Novel Secure Image Steganography Using Improved Logistic Map and DNA Techniques

A . IMAGE STEGANOGRAPHY AND DATA HIDING IN QR CODES

In this technique data is put in QR code for the alleviate of entrée of conveyance information[1].
For the protection of data , AES algorithm is used to encrypt the data and then image and data is hidden using DWT and LSB steganography techniques .

1. QR Code :-

QR codes are 2 dimensional matrix. Large volume of unique data is stored in it. Bar-codes are one dimensional vector. QR codes are having more storage capacity then the bar code. QR codes can seize up to 7,089 numeric characters and up to 4,296 alphanumerical letter values.

2. Discrete Wavelet Transformation (DWT):-

DWT is a mathematical tool for analytically decomposing an image. It is useful for processing of moving signals. Small waves are used for the modifications which are known as wavelets, of different frequency and for limited time period. the image is process by 2-D filters in both dimensions. They decompose the input image into four parts. These parts are non-intersecting or multi-resolution sub-bands LL1, LH1,HL1 and HH1. The sub-band LL1 shows the coarse-scale Discrete Wavelet Transform (DWT) coefficients and remaining sub-bands as LH1, HL1 and HH1 indicate fine scale of DWT coefficients.

3 . Method:-

To store every record of particular criminal QR code is used . The confidential data is hidden in the image before embedding in image which is encrypted using AES algorithm. Data is hidden in image by using DWT technique and in DWT data is hidden in the HH band.

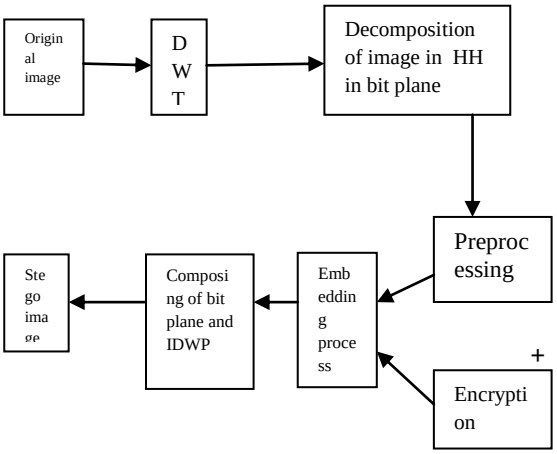


Fig no-1

This technology can be used in protecting the criminal data. The criminal information may be modified for deceptive the police department. The data that can be altered or erased is mainly the type of crime performed, which can be altered for dropping the chastisement of the criminal. This technique can stop the unofficial entrée and modification in record.

B. IMAGE STEGANOGRAPHY FOR CRIMINAL CASES

"Image Steganography for Criminal Cases" system can be used to hide data inside an image, and send it securely[2].

It uses two layers of protection to preserve the solitude, secrecy and correctness of the data. Following Figure shows the skeleton for the on the whole process of the system. The system is proficient to conceal the data within the image and take back the data from the image.
From Figure 2 ,for hiding the data, a username and password is obligatory former to using the system. Once the addict has signed into the system, the addict
can employ the information (data) mutually with the undisclosed key to veil the data inside a elected image. Using this technique data is set in and concealed within the image with nearly zero deformation of the cover image.

The secret key in this algorithm played an necessary function ,By using this key user can access the secret data . The key is robotically generated by system. Key is generated by using Advanced Encryption Standard (AES) . Within the image coded data is hidden data cannot be revive back lacking of key. Once the coded data is hidden within the image, this data can be retrieve back from the stego-image.

Ist layer contain -

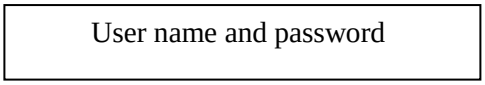


Fig no-2

Second layer contain -

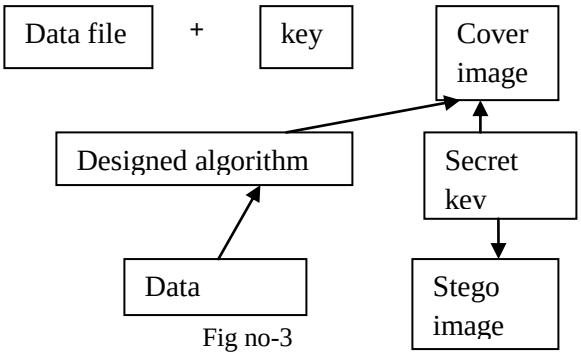


Fig no-3

C. BLUETOOTH PAIRING USING STEGANOGRAPHY

Bluetooth is a WPAN, which is proficient of spread data whether data is audio or video at a rate of 24 Mbps. Several devices can unite at a time to share data lacking any wired connection[3]. But it is not much secure to send data using Bluetooth. MITM attack can be possible using the Bluetooth. In this attack attacker secretly relays and possibly modifies the communication between two parties who think that they are directly associated. Using steganography if data is shared than this attack can be over come . In this technique connection is established using steganography and after that data is being send out.

1 . Method

The method is devoted for ansure a secure pairing by three distinct phases, which are defined in their incident order:

a) In first phase key is generated and set into a cover image. This key is sent to the second party. Second party receive the image and he also generate a key.Then, this key sent back to the producer. This process does not require any user interaction.

b) In second phase key is retrieved from the image and a share key is generated. Generation of share key make communication more secure .Connection is established by verification process

which is initiated before the generation of share key. All verification processes are internal means user interaction is not needed.

c) In last phase connection is establed by sharing the shared key. This phase is the final phase before the successful connection establishment. All verification processes are internal means user interaction is not needed.

This technique revise the current standard of pairing process and formulate a novel pairing structure based on steganography.

D. SECURE IMAGE STEGANOGRAPHY USING IMPROVED LOGISTIC MAP AND DNA TECHNIQUES:-

1. The Logistic Map

Logistic map is one of the way to obtain chaotic sequence . it is a simple way to obtain chaotic sequence among other ways[4]. The interval of values varies from [0,1]. A dynamic nonlinear equation is used to show chaotic
behavior. The equation of logistic mapping is defined as Equation (1):

$$xn + 1 = \mu . xn . (1 - xn) \quad (1)$$

Here $0 < xn < 1$ and μ is a control parameter or a bifurcation parameter. $\mu = 4.0$ has the most flat, uniform and symmetric histogram

B. The Improved Logistic Map

The superior logistic map is defined as Equation (2)

$$Xn+1 = \begin{cases} \mu . Xn . (1- Xn) & Xn < 0.5 \\ \mu . Xn . (Xn -1) + \mu / 4 & Xn \geq 0.5 \end{cases} \quad (2)$$

DNA contain two twisted strands which stores the genetic information. Information is in four nucleotides:- a) Adenine

b) Cytosine
c) Thymine
d) Guanin

A and G is complement with T and C . Binary values are used to represent these A,G,T and C[5,6]. This method introduced 15! Complementary rules which are 6 in previous method and these rules are known as Watson Crick base pairing. In this method confidential image is changed into DNA matrix by using mapping rules .Matrix is transformed in to 1-D bit stream and these streams are scrambled by using logistic function. Two bits are hide in edge of pixels of carrier image.

1. Method

a) Read cover image and use canny edge detection algorithm to detect the boundaries of host image.
b) Use improved logistic map upto 300 times to avoid transit effect until the key in logistic function become 1.
c) Choose mapping rule after calculating the key which is in interval.
d) DNA matrix is obtained according to the complementary mapping rule. Convert matrix in 1-D bit stream and scrambled them using chaotic sequence generated by new logistic map.
e) 2 LSB's of edge pixels are replaced by 2secret bit.
f) Stego image is obtained by this process.
g) Original message at receiver end can be obtain by reverse the process

CONCLUSION

This paper is giving an overview of current technologies that are using steganography . In this paper four technologies are discussed which are used to hide the data with in a image. first two technologies can be used to send confidential data or in crime investigating branches to send the confidential file or data with in a image[1,3]. Next two can be used to send the secret data without interruption of mediator[4,5]. Steganography is a vast area and many new researches can be done in this field.

REFERENCES

[1]. Rutuja Kakade, Nikita Kasar, Shruti Kulkarni, Shubham Kumbalpuri, Sonali Patil, Student, Associate Professor, Dept.of Computer Engineering, PCCOE, Maharashtra, India" Image Steganography and Data hiding in QR Code" International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 05 | May -2017, e-ISSN: 2395 -0056.

[2]. Divya Suryawanshi, Meetali Salvi, Soumya Pandey Terna Engineering College, Nerul, Navi Mumbai IT Department, Mumbai University, Image steganography for criminal cases, Volume 5, Issue 2 | ISSN: 2321-9939

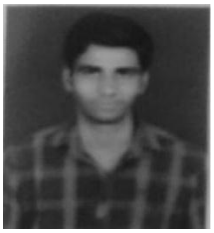
[3]. Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen University of Eastern Finland, School of Computing, Kuopio Campus, " A novel method for bluetooth pairing using steganography"International Journal on Information Technologies & Security, № 1 (vol. 9), 2017

[4]. Shuliang Sun,School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University, China," A Novel Secure Image Steganography Using Improved Logistic Map and DNA Techniques" researchgate.net/publication/317829911, Article · May 2017.

[5]. S. U. Maheswari and D. J. Hemanth, "Different methodology for image steganography-based data hiding: Review paper," International Journal of Information and Communication Technology, vol. 7, issue 4/5, pp. 521-536, 2015.
[6]. X. Wangand and D. Luan, "A Novel Image Encryption Algorithm Using Chaos and Reversible Cellular Automata, Communications in Nonlinear Science and Numerical Simulation, Vol. 18, No. 11, pp. 3075-3085, November, 2013.
[7]. S.K. Yadav, Manish Dixit Dept.of Computer Engineering, Madhav Institute of technology and science, Gwalior, India "A comparative study for image steganography using Transformation Domain method" International journal of science and Engineering(IJCSE), Volume: 05 Issue: 06 | Jun -2017.
[8]. Rajesh Shah, Yashwant Singh Chouhan Christian eminent college, Indore (M. P.)India" Encoding of Hindi Text Using Steganography Technique" International Journal of Scientific Research in Comp c Research in Computer Science and Engineering Science and Engineering Science and Engineering Research Paper Vol-2, Issue-1 E-ISSN: 2320-7639

Authors Profile

kirti done B.Tech from V.C.E.Rohtak in I.T. 2014 and M.Tech from University institute of Engg. And Technology in C.S.E 2016. Currently working in maa sarawati institute of engg. And technology since 2017She has published two papers one review and other research paper.



Parmod sarowa done B.Tech from Bhagwan parsuram college of engg. gohana in E.E. 2013 and M.Tech from R.N. of Engg. And Technology in E.E. 2016. Currently working in maa sarawati institute of engg.and technology since 2017. He has ublished two papers one review and other research paper.

