International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

RESEARCH ARTICLE

ISSN: 2321-7758

A PSEUDO-RANDOM LSB IMAGE STEGANOGRAPHY TECHNIQUE BASED ON CHAOS

RUCHI GUPTA[1], DHARAMBIR SINGH[2], BHAWNA RAO[3]

[1,2,3]M.Tech Research Scholar, SITM Rewari, Haryana, India

RUCHI GUPTA

DHARAMBIR SINGH

BHAWNA RAO

ABSTRACT

Steganography is the science of camouflaging message, video, image or any other da within another file, which can be any multimedia file. The purpose of this technique is hide the existence of the message in cover file from unauthorized party. It takes t advantages of limited perception of human to observe subtle changes in images, sou etc. Here our concern is about digital images as they are more frequent over tl internet. In spy/hacker world Steganography and Cryptography are cousir Cryptography alters a message so it cannot be understood whereas Steganography hid the message so that it cannot be read. There are lots of Steganography techniques bas on digital images like LSB (Least Significant Bit), in this techniques some bits of digi cover image get inverted when some input or alteration in image element.Analy pseudo random techniques and to propose a Pseudo-Random LSB Steganograp technique where chaotic map is used to generate random numbers. In the propos mechanism instead of using pseudo random generator which is less variant we ha used chaotic maps technique to obtain the random sequence

KEYWORDS- Steganography, Communication, Carrier, Digital Image, Cryptography, LSB, Random numbers logic

1. INTRODUCTION

The word Steganography is a combination of two Greek words Steganos, which means secret and covered and graphy means drawing and writing. The goal of Steganography is to hide data and messages inside other harmless messages in a way that does not allow any unauthorized person to even detect that there is a second secret message present [2]. The process of Steganography required a proper media to hide data inside it so that it can keep data undetectable from hackers/ attackers. The size of media which contains secret data plays vital role as one can easily detect it because of unusual size, as the size of media increases the possibility of its detection directly get increased. That's why Steganography techniques are usually used for hiding data in fixed sized media [7].

Now a day, there are several Steganography techniques used by technicians for data hiding such as [1]:

- Permutation Steganography.
- Least Significant Bit (LSB).
- Bit Plane Complexity Segmentation (BPCS).
- Chaos Based Spread Spectrum Image Steganography (CBSSIS).

The basic model of Steganography consists of Message, Password and Carrier. Carrier is also

known as cover object in which message get embedded.

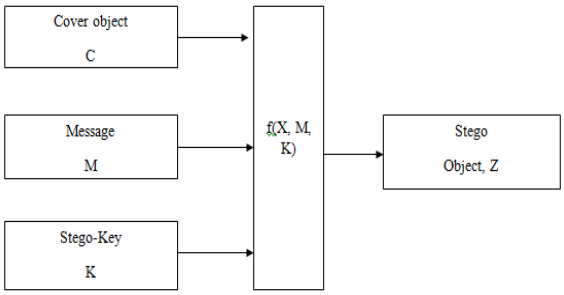

Figure 1 Basic Model of Steganography.

Message M, is the data which the sender wishes to remain in confidential form, it may be in simple text, cipher text, digital images or in any other multimedia form. The message can be anything that can the embedded in a stream of bit such as water mark and copy right mark or a serial number etc. Password is commonly known as stego-key K, is used to ensure that the only recipient to know the corresponding decoding key would be able to extract the message from the cover object C. The cover object in combination with message M is known as stego-object, Z. On the counter part, for recovering messages is from a Stego-Object Z requires the cover object C as well as the decoding key if a stego-key was used during the encoding process [10]. In some application there is no need of original image to extract the message there may be following cover object which can be used as suitable carriers:

- Networking Protocols such IP, UDP and TCP.
- Audio files in different formats like WAV, MIDI, MPI, AVI, VOC and MPEG.
- Disk such as FDD, Pen Drive and other Flash drives.
- Digital Image in both grey-scale and colour format such as bmp, .jpg and gif [3].
- Steganography has void range of applications in different areas like [8]:
- Validation: The way of finding Uniqueness.
- Solitude: used to conform that the message has reached to required receiver.
- Integrity: it prevents message alteration.
- Non-repudiation: it certifies that the message is authentic.

2. A PSEUDO RANDOM LSB IMAGE: In this process of encoding method, a random key is used to randomize the cover image and then hide the bits of a secret message into the least signi_cant bit of the pixels within a cover image. The transmitting and receiving end share the stego key and random-key. The random-key is usually used to seed a pseudo-random number generator to select pixel locations in an image for embedding the secret message [4].

1) Read character from text file that is to be hidden and convert the ASCII value of the character into equivalent binary value into an 8 bit integer array.
2) Read the RGB colour image (cover image) into which the message is to be embedded.
3) Read the last bit of red pixel.
4) Initialize the random key and randomly permute the pixels of cover image and reshape into a matrix.
5) Initialize the stego-key and XOR with text file to be hidden and give message.
6) Insert the bits of the secret message to the LSB of the Red plane's pixels.
7) Write the above pixel to Stego Image file [13].

Extraction of Hidden Message

In this process of extraction, the process first takes the key and then random-key. This key takes out the points of the LSB where the secret message is randomly distributed [5]. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the stego-key.

1) Open the Stego image file in read mode and from the Image file, read the RGB colour of each pixel.
2) Extract the red component of the host image.

3) Read the last bit of each pixel.
4) initialize the random-key that gives the position of the message bits in the red pixel that are embedded randomly.
5) For decoding, select the pixels and Extract the LSB value of red pixels.
6) Read each of pixels then content of the array converts into decimal value that is actually ASCII value of hidden character.
7) ASCII values got from above XOR with stego-key and gives message file, which we hide inside the cover image [9].

In chaotic base the embedded message is concealed on to the cover image at the chaotic map base randomly generated pixel values before transmitting. After transmitting the stego-image it is then decrypted at the receiver's side by using the same key to obtain the original message back.

3.CHAOTIC SIGNAL

The chaotic signals are like noise signals but they are completely certain, that is if we have the primary quantities and the drawn function, the exact amount will be reproduced. The advantages of this signal are as follows [12, 13]:

3.1 THE SENSITIVITY TO THE PRIMARY CONDITIONS: This means a minor change in primary amount will cause a significant difference in subsequent measures. It means if we have a little change in the signal amount, the final signal will be completely different.

3.2 THE APPARENTLY ACCIDENTAL FEATURE: In comparison with productive accidental natural number in which the range of the numbers cannot be produced again, the technique used for producing the accidental number in algorithm based on the chaotic function will prepare the ground that if we have the primary quantities and the drawn function, we can produce the numbers again. The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique [6]. The most common technique of secure the digital images is to scramble the digital data such that original message of the documents should not be known. There are several approaches to achieve this for example Steganography, compression, digital watermarking and cryptography. In this paper we focus on the encryption techniques of digital image based on the chaos mapping. Basically image encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key and the transforming information using "encryption algorithm" into a form that cannot be deciphered without a decryption key. On the other hand, decryption OF image retrieves the true information from the encrypted form image. There are several digital image encryption systems to encrypt and decrypt the image data, and there is not available the single encryption algorithm that satisfies the different image types. The encryption techniques based on the chaos mapping provides the encrypted digital images to hold the multilevel encryption method and also decreases the computational complexity of the encryption process. Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption [13]. The encryption techniques based on the chaos have different types of applications in various areas for examples the internet communication, military, health care, mapping and positioning, picture messaging applications on cell-phones, multimedia systems, medical imaging, Tele-medicine, privacy and government documents etc. The evolution of image encryption process is moving towards a future of endless possibilities. Everyday new

methods of encryption techniques are discovered [11].

It includes generation of random sequence for various 1D and 2D discrete maps based on mathematical equations and relations i.e. Logistic map, Cubic map, Ricker's map, Sin map, Henon map, Gingerbreadman map, Burgers' map, Tinkerbell map, etc. One of the most studied examples of a one-dimensional system is logarithmic map, its properties and chaotic performance is also similar to logistic map. Its equation is

Logistic Map equation =Alog * log(xn) * (1- log(xn))

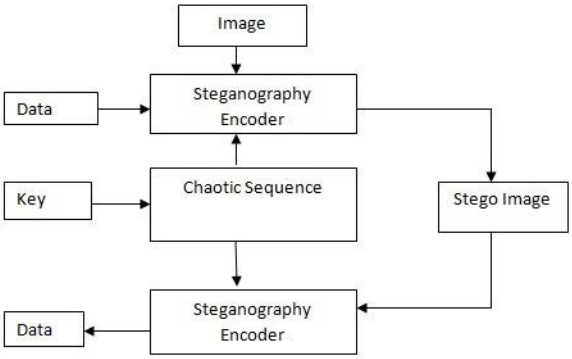

Fig 2 Block diagram of Pseudo Random Chaotic base Steganography

4ALGORITHMS

4.1 EMBEDDING MESSAGE ON COVER IMAGE:

1. Get the message to be embedded and the cover image on which this message is to be embedded.
2. Convert the message into bits i.e. binary form.
3. 3. Generate random numbers (using key) based on chaotic maps as per the size of the cover image i.e. 1≤ random number ≤ total no. of pixels
4. Now using LSB Steganography place the data bit by bit at the randomly generated places.

4.2 RETRIEVING ORIGINAL MESSAGE:

1. Obtain the same random sequence i.e. at the sender's side using the same key of transmitter.
2. Now with the help of the sequence, convert respective pixel values into the binary form.
3. Combine the LSB of these pixels to obtain the original message.

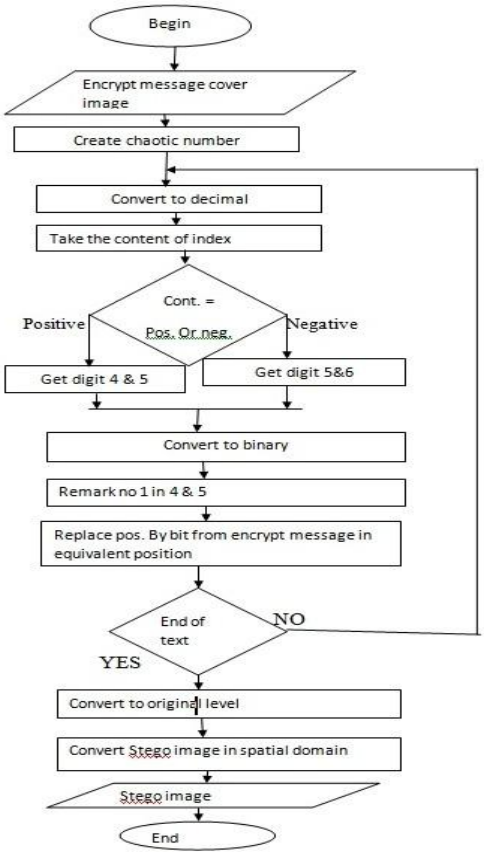

Fig 2 Flowchart of hiding text information into cover image

Algorithm:

1. Begin
2. Giving a cover image whose size is M*N
3. Using chaotic map to create random number
4. Convert random number in decimal.
5. Take the content of index in image.
6. Check if the number is negative, get the digit 5 & 6 else get digit 4 &5.
7. Convert these two digit in equivalent binary number.
8. Remark the position of one in digit 4 if number is negative, or digit if number is positive .
9. Replace the position of ones in digit 4&5 secret text in equivalent position in digit 5 or 6.
10. Repeat the text until the end of encrypted text

11. Convert the level to original place in image.
12. Convert the image to spatial domain.
13. End
14. Output –Stego image

4. CONCLUSION

Steganography is covering wide range of area of digital world by providing useful applications to all. It has its vital role in defence, terrorism and in other means of secret communications. We have discussed about various parameters related to Steganography like its applicability on various Experiments for improving the steganalysis performance and also analyzing the hiding capacities of the existing research work. The steganalysis performance of state-of-the-art detectors is near-perfect against current Steganography schemes. A novel, robust and secure hiding schemes that can resist steganalytic detection must be implemented. Hiding schemes are characterized by three complementary requirements- security against steganalysis, robustness beside distortions in the transmission channel, and capacity in terms of the embedded method. In our randomized LSB technique we have embedded two bits in a pixel using a message dependent randomized approach. In future we would like to exploit the possibility of hiding three bits in moderate bit locations in a randomized manner without disturbing the least significant bit in each pixel. The possibility of embedding by changing every pixel value with a new one which will conceal the hidden data can also be exploited. LSB substitution methods give high capacity, whereas Chaotic methods give high security. Some techniques are already available which combines both the LSB and Chaotic approaches to get both high capacity and high security. However, better techniques are always warranted through the combination of both LSB and Chaotic approaches which can address the short-comings in the previously existing techniques.

REFERENCES

[1]. A.K. Jain and U. Uludag, “Hiding Biometric data”, IEEE, 25:1494-1498, Nov. 2003.

[2]. Cachin, “An information-Theoretic Model for steganography”, in proceeding 2nd Information hiding Workshop, vol. 1525.

[3]. D.Artz, “Digital Steganography: hiding Data within Data”, IEEE Internet Computing, pp. 75-80, may-jun 2001.

[4]. IBBeMndeSry, s Wtem., sDJ.oGurrnuahll,, vaonld. 3N5.,nMoo. r3i4m, o1t9o9, 6“,T pepc.h 1n3iq1u-3e3s 6f.o r data hiding”,

[5]. I”mDaegteecst”inJgessLicSaBFrSidterigcahn ,oMgrairpohsyla vi nGoCljaonlo, r anadndRuGir Dayu- SSctaatlee University of New York, Binghamton.

[6]. IPmo-aYgeu e hSteCgahneong, raHphuyn”g -IJnuternLainti,o”nalA J ouDrWnaTlofBAaspepdliedApSpcrioeancch eafnodr Engineering 2006. 4, 3: 275-290, ISSN 1727-2394. PP. 275-290.

[7]. N. Provos, P. Honeyman, “Hide and Seek: An introduction to Steganography”, IEEE SecurPriv, 2003, 1(3): 32-44.

[8]. N. F. Johnson and S. Jajodia, “Steganography: Seeing the Unseen”, IEEE, 1998.

[9]. M.-H. Yang, D. J. Kriegman, and N. Ahuja, “Detecting faces in images: A survey”, IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 1, pp. 34–58, Jan. 2002.

[10]. Ruchi and V. Goyal, “Image Steganography Combined with TSFS using LSB”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 8, August 2015.

[11]. SMtedg. anoJgarkaiprhHyossWaiinth, Pse“uIdnoforarnmdaotmio n-PHeirdminugtatioUn”sinBganglIamdaegsheI Rsessueea: r3c,h P aPgueb:l 2ic1a5ti-o2n2s5 , JJoaunrunaarly, -I FSeSbNru:1a9ry9,8 2-2001043. ,P PV. o2l1u5m-2e:2 59. ,

[12]. X. Xie, J. Lai and others “Extraction of illumination invariant facial features from a single image using nonsubsampledcontourlet transform”, Elsevier, Pattern Recognition 43, 2010.

[13]. W. Zhao and R. Chellappa, (Eds.), "Face Processing: Advanced Modeling and Methods,"Elsevier, 2006

Ms. Gupta pursuing herM.tech in Computer science And Engineering From SITM Rewari,she has his bachelor of technology from Gurgaon College Of Engineering for Women Gurgaon, Haryana, India in Computer Science And Engineering. Currently she is pursuing Research in Human Behaviour Modelling using Artificial Intelligence.

Mr. Singh pursuing his M.tech in Computer science And Engineering From SITM Rewari, he has his bachelor of technology from Dronacharya College Of Engineering Gurgaon, Haryana, India in Computer Science And Engineering. Currently he is pursuing Research in Steganography. He has published a research papers in reputed International Journals.

Ms. Rao currently pursuing her M.tech from SITM Rewari, Haryana, India. She has his bachelor of technology from Vaish college of engineering, Rohtak, Haryana, India in Computer Science And Engineering currently she is pursuing Research in Sentiment Analysis.

GUIDE- ANJALI NAMDEV(Head Of Department CSE Somany Institute Of Technology and Management)