An Extensive Review on Substitution Steganography with Security Improved Encryption

Subodh Sharma[1], Prof. Angad Dixit[2]

[1]Mtech. Scholar, [2]Research Guide

Department of IT, NIIST, Bhopal

Abstract- Steganography is a science or art widely used to communicate securely for secret information sharing. It is the data hiding technique used for embedding/encoding secret information or data in such a manner that the existence of the information is hidden. Steganography is a method to shroud information inside a cover medium in such that the presence of any communication itself is imperceptible rather than cryptography where the presence of secret communication is known but is indecipherable. Data transmissions are essential and turned into a need these days. Whether people share their private messages with his/her close friends, or business secrets with their partners, they must protect their confidential information from hackers, third person, or competitors. Steganography is also utilized for the less dramatic purpose of watermarking. The applications of watermarking mainly involve the protection of intellectual property such as ownership protection, file duplication management, document authentication. This work presents an examination and analysis of security improvement of chaotic image using substitution stegnography.

Keywords- Security Analysis, Chaotic Encryption, Image Encryption, Substitution Steganography, Security Improvement.

I. INTRODUCTION

The word steganography originally came from a Greek word which means “concealed writing”. Steganography has an edge over cryptography because it does not attract any public attention, and the data may be encrypted before being embedded in the cover medium. Hence, it incorporates cryptography with an added benefit of undetectable communication. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data

In digital media, steganography is similar to watermarking but with a different purpose. While steganography aims at concealing the existence of a message with high data capacity, digital watermarking mainly focusses on the robustness of embedded message rather than capacity or concealment. Since increasing capacity and robustness at the same time is not possible, steganography and watermarking have a different purpose and application in the real world. Steganography can be used to exchange secret information in a undetectable way over a public communication channel, whereas watermarking can be used for copyright protection and tracking legitimate use of a particular software or media file.

Image files are the most common cover medium used for steganography. With resolution in most cases higher than human perception, data can be hidden in the “noisy” bits or pixels of the image file. Because of the noise, a slight change in the those bits is imperceptible to the human eye, although it might be detected using statistical methods (i.e., steganalysis). One of the most common and naive methods of embedding message bits is Least Significant Bits (LSB) replacement in spatial domain where the bits are encoded in the cover image by replacing the LSB of pixels [1]. Other techniques might include spread spectrum and frequency domain manipulation, which have better concealment properties than spatial domain methods. Since JPEG is the most popular image format used over the Internet and by image acquisition devices, I use JPEG as the default choice for steganography.

Steganography is an alternative method for privacy and security. Instead of encrypting, we can hide the messages in other innocuous looking medium (carrier) so that their existence is not revealed. Clearly, the goal of cryptography is to protect the content of messages, steganography is to hide the existence of messages. An advantage of steganography is that it can be employed to secretly transmit mes- sages without the fact of the transmission being discovered. Often, cryptography and steganography are used together to achieve higher security.

Figure 1.1 shows a simple representation of the generic embedding and extraction operation in steganography. During the embedding operation, a message is inserted into the medium by altering some portion of it. The extraction oper- ation involves the recovery of the message from the medium. In this example, the message is embedded inside a carrier and is transmitted via a public channel (e.g., internet). While at the receiving site, the message is extracted using the key shared between the sender and receiver. The message is the hidden information and can be a plain text, cipher text, image or anything that can be converted into stream of bits.

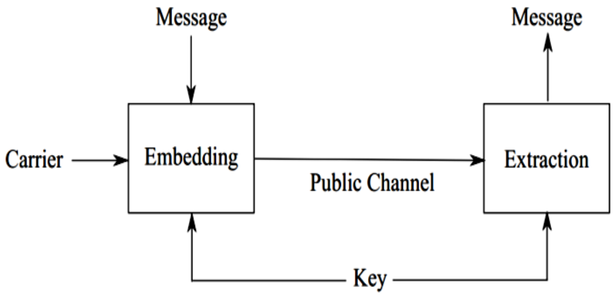

Figure 1.1 General model of steganography.

Applications of Steganography

- Secret Communications The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.
- Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
- Copyright Protection Copy protection mechanisms that prevent data, usually digital data, from being copied.The insertion and analysis of water- marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

II. CHAOTIC IMAGE ENCRYPTION

To gain a consistent method for encryption has been always in need even all over the past. Several encryption applications are in an assortment from defense and intelligences utilize in profitable undertakings on daily basis. An expertise has enhanced to take into account simpler and improved encryption and transmission, hence it has also permitted the development in interception and cryptanalysis. Codes have been turn out to be further progressive, developing from simple character replacement ciphers to today’s algorithm of large pseudo-primes, exponents, and particular consistency.

In any case the idea has stayed basic; it is anticipated to have the capacity to send data starting with one point then onto the next without any one having the capacity to comprehend it in the mid. The appearance of the web has made security of information and assurance of protection a significant reason for concern toward anybody. The profoundly eccentric and irregular look nature of chaotic signals is the most tempting feature of deterministic chaotic system that may prompt to as novel applications. With the quick advancement of the computer innovation and data processing technology, the issue of data security is constantly more imperative. Data hiding away is normally used to secure the imperative data from unveiling when it is transmitting over an uncertain channel. Computerized image encryption is a standout amongst the most vital systems for image data.

The image encryption methods chiefly incorporate compression approach, cryptography system, chaos strategies, and DNA procedures etc. Cryptography and chaos have some regular peculiarities, which is debated in consequent segment. With the progression of portable correspondence technologies, the usage of varying audiovisual data in account with textile data gets to be more common than the past. Cryptography methodologies are in this way essential for storage of secured media content and circulation over open systems, for example, the web. A conventional approach to oppose statically and differential cryptanalysis is to utilize transformation and dispersion on the other hand.

Chaotic cryptography depicts the utilization of chaos hypothesis (specifically physical dynamical systems working in chaotic administration as a component of correspondence methods and processing algorithms) to accomplish diverse cryptographic assignments in a cryptographic system.

The ability of creating truly perplexing examples of conduct is an astonishing characteristic of chaotic systems. This is carried out from straightforward genuine systems or in recreations from low dimensional systems given by a little set of development mathematical equations. This quality has made them especially valuable for application in a wide variation of restraints, for example, science, commercial concerns, engineering and others [35][36]. Chaotic systems are utilized to create, reproduce, support or control diverse techniques enhancing their execution or giving a more suitable yield, in these sort of applications.

A distinctive structural design of prevailing chaos-based image cryptosystems is presented in Fig 2.1.

1. It comprises of two phases, namely; confusion and diffusion phases. In the confusion phase, permutations of image pixels are prepared in a secret demand, deprived of varying their values. The purpose of the diffusion phase is to alter the pixel values in sequence so that a small alteration in one pixel is blowout out to several pixels, with looking forward to the whole image. To disassociate the affiliation among adjacent pixels, the confusion phase is performed n times, where n is usually larger than 1, monitored by the diffusion phase. The comprehensive n-round confusion and single round diffusion replicate from times, with m typically higher than 1, so as to acquire a

satisfactory level of security. The constraints of the chaotic maps primary to the permutation and the diffusion should better be unrelated in diverse rounds. This is achieved by a round key generator with a seed secret key as input.

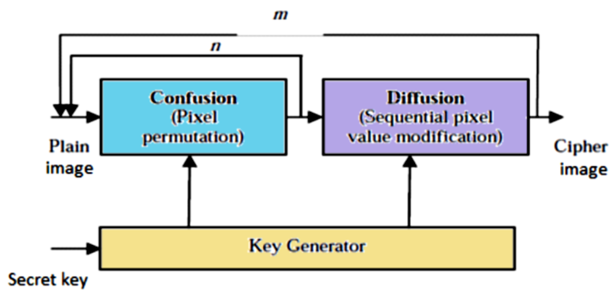

Figure 2.1 Chaos Based image encryption systems.

There is a set of features that encapsulate the characteristics perceived in chaotic systems. These are deliberated as the mathematical standards that define chaos. The most appropriate ones are:

- Dynamic instability: Also mentioned as butterfly effect, it is the property of sensitivity to preliminary state of affairs, where two randomly closed preliminary situations progress with considerably dissimilar and deviating trajectories.
- Topological mixing: spontaneously represented as mixing colored dyes, which explains that the system will progress in time so that any specified section of states is constantly converted or overlaps with any other specified section.
- A periodicity: the system progresses in an orbit that on no occasion replicates itself, that is, these orbits are never periodic.
- Dense periodic orbits: it explains that the system follows a dynamics that can diligently approach every potential asymptotic state in random.
- Ergodicity: arithmetical capacities of the variables give related outcomes no matter if they are executed over time or space. Other way around, the dynamics indicates alike statistics when measured over time or space.
- Self-similarity: the progression of the system, in time or space, demonstrates the similar presence at dissimilar scales of observation. This distinguishing feature creates the system to appear auto- repetitive at dissimilar scales of observation.

III. LITERATURE REVIEW

SR. NO.	TITLE	AUTHOR	YEAR	APPROACH
1	Substitution steganography with security improved by chaotic image encryption,	J. Oravec and J. Turán,	2017	Author describes an information hiding scheme, which combines advantages of steganography and cryptography in this examination.
2	Stego integrated image encryption using row and column indexing — An information security,	P. Praveenkumar, R. S. Devi, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan	2017	Image encryption using various strategies in order to improve the rate of security has been adopted by author.
3	A Steganography System Based on Dual Chaotic Encryption and Singular Value Shifting,	J. Miao, Y. Xiao, Z. Su and Y. Liang,	2016	Author utilizes the advantages of dual chaotic mapping in randomness, complexity and safety to encrypt plain texts.
4	Prediction error and histogram shifting based reversible data hiding,	P. Tamilselvi and M. Manikandan,	2015	Author improve the security for multimedia files and to increase the volume of hidden data in an image.
5	Improved reversible data hiding using histogram shifting method,	A. K. Mohan, M. R. Saranya and K. Anusudha,	2015	A reversible data hiding (RDH) algorithm with improved security reported by author
6	An algorithm for enhanced image security with reversible data hiding,	A. K. Mohan, M. R. Saranya and K. Anusudha,	2014	A novel reversible data hiding algorithm with improved security is reported by author
7	Study on Image Encryption Algorithm Based on Chaotic Theory	Q. Zhang,	2013	Studies about the image encryption algorithm based on chaotic theory is reported by author

J. Oravec and J. Turán, [1] This article describes an information hiding scheme, which combines advantages of steganography and cryptography. After brief review of currently used techniques and their properties, a chaotic image encryption method based on quadratic map is proposed. This algorithm is then utilized as a tool for encryption of image representing secret data, which is afterwards embedded into cover image by means of LSB matching. Examination also provides verification of results achieved by both parts of presented approach and discusses its advantages and drawbacks.

P. Praveenkumar, R. S. Devi, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan [2] Multimedia is the ruler of the digital era and here data storage and transmission is of utmost importance. Data transmission is the prime focus of the Information industry. And how to ensure this safely has become a crucial issue. This brings in the need for protection of data in other words, privacy. As a user, protection against misuse of private information is essential and hence several encryption strategies have evolved. In the proposed scheme, image encryption using various strategies in order to improve the rate of security has been adopted. The methods involved are row and column shuffling, indexing, swapping, wavelet transforms and watermarking. Stego involves hiding a message in a stego medium whereas water marking is used to prove one's copyright protection. The resultant crypto image data is highly secure and it improves the imperceptibility of the encrypted image.

J. Miao, Y. Xiao, Z. Su and Y. Liang [3] Information security has been given increasingly attention especially in multimedia related fields, and how to ensure transmission safety of confidential information is a significant and challenging problem. We build a system combing dual chaotic encryption of texts and information hiding technique based on a modified maximum singular shifting method with images as carriers. We utilize the advantages of dual chaotic mapping in randomness, complexity and safety to encrypt plain texts. Conventional steganography is advanced by introducing outstanding properties of SVD into our system so that robustness and imperceptibility are largely improved. Experiments demonstrate that system performs well both in robustness and image visual effect.

P. Tamilselvi and M. Manikandan, [4] Objective of this work is to improve the security for multimedia files and to increase the volume of hidden data in an image. The technique of reversible data hiding is capable of recovering the data embedded and the original image from a stego image without distortion. For some applications such as satellite and medical images, reversible data hiding is the valuable solution to render copyright or authentication. Reversible data hiding scheme is done based on Modification of Prediction Error (MPE). In this proposed MPE method, the histogram of prediction errors modified to prepare vacant positions for data embedding based on the secret data length. So data hiding capacity of an image is increased. The PSNR and embedding capacity of the stego image produced by MPE is more when compared to other techniques. To increase security, the secret data is encrypted using chaotic encryption algorithm. The encrypted secret message is then hide into the image. The complexity of extracting the encrypted secret data from the stego image is more. It is impossible to decrypt the data even though it is hacked. The encryption key generated is based on secret data and chaotic sequence. This improves the security of the multimedia files.

A. K. Mohan, M. R. Saranya and K. Anusudha,[5] A reversible data hiding (RDH) algorithm with improved security, which can reacquire the cover in separable manner from the marked stego-image is presented in this exploration. In the content owner side cover image is encrypted by deploying user-defined security key derived-chaotic based transposition algorithm. Then the data hider conceals secret data into the encrypted image by perturbing its histogram, by utilizing another user defined data hiding key. At the receiver side, the recuperation of the cover can be implemented directly or indirectly which depends on shared key. Lower bound of Peak Signal to Noise Ratio (PSNR) for direct recuperation method is set to 48.13dB. This technique has improved security & achieved higher data hiding capacity than the existing methods.

A. K. Mohan, M. R. Saranya and K. Anusudha, [6] A novel reversible data hiding algorithm with improved security, which can recover the original image in separable manner without any distortion from the marked image after the hidden data have been extracted, is presented in this exploration. In the content owner side image is encrypted by key derived chaotic based transposition algorithm. The data hider then hides some data into the encrypted image by histogram modification based data hiding, making use of data hiding key. At the receiver side, if the receiver has only encryption key, then the decrypted image with high similarity with cover image can be obtained, but cannot read the hidden data. Lower bound of Peak Signal to Noise Ratio (PSNR) of this method is much higher than the existing methods (48.13dB). If the receiver has only data hiding key, then the hidden data can be extracted out, but cannot read the content of the image. If the receiver has both keys, he may first extract the data using data hiding key and then decrypt the image using encryption key. The method also has a higher data hiding capacity than the existing reversible data hiding techniques in encrypted image.

Q. Zhang, [7] With the rapid development of high-tech such as the cloud technology, information security has become more critical than before, so the cryptography assunes a key technology in information security. Recently, some new cryptography theories have attracted increasing attention under the background of research on algorithm efficiency and security has become the current hot research topic. Chaotic algorithm is very suitable for stream cipher encryption not only for its sensitivity to initial conditions for time series generated but also for its complex structure which is difficult to analyze and forecast. At the same time, it can provide smart pseudo random sequence with excellent randomness, correlation and complexity. This research work mainly studies about the image encryption algorithm based on chaotic theory.

IV. PROBLEM FORMULATION

Since the discovery of the existence of such chaotic systems and the increasing number of the applications they are involved in, especially in communication engineering , researchers have been proposing many circuit implementations and optimization techniques for chaos generators. The majority of such chaos circuit implementations are focused on analog designs. In general, analog circuit implementations of chaos generators are sensitive to the operating conditions, process variations and temperature. Furthermore, the fact that these analog implementations are realized by using capacitors makes such chaos generators area inefficient and also initial conditions cannot be set accurately. These limitations make the digital implementation of chaotic systems desirable, since they overcome such issues.

V. CONCLUSION

This study introduces a analysis of chaos-based image Steganography to enhance the system perfrmance and to insure better security level. Steganography is an effective way to hide and secure sensitive information. Steganography has been mostly used in historical times and the present day. In World War II, French utilized the invisible ink to send messages. Steganography has also been used in recent times to hide data inside images and post those images on a common website so that the relevant receiver can download the image and extract the secret message. This examination focuses on the approach to enhance system performance like increasing the security of the message and increasing PSNR and reducing the distortion rate. This examination focuses on the analysis and development of effective steganography techniques which can hide data with a low detection rate and high payload.

REFERENCES

[1]. J. Oravec and J. Turán, "Substitution steganography with security improved by chaotic image encryption," 2017 IEEE 14th International Scientific Conference on Informatics, Poprad, 2017, pp. 284-288.

[2]. P. Praveenkumar, R. S. Devi, K. Thenmozhi, J. B. B. Rayappan and R. Amirtharajan, "Stego integrated image encryption using row and column indexing — An information security," 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2017, pp. 1-4.

[3]. J. Miao, Y. Xiao, Z. Su and Y. Liang, "A Steganography System Based on Dual Chaotic Encryption and Singular Value Shifting," 2016 6th International Conference on Digital Home (ICDH), Guangzhou, 2016, pp. 6-10.

[4]. P. Tamilselvi and M. Manikandan, "Prediction error and histogram shifting based reversible data hiding," 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), Chennai, 2015, pp. 1-5.

[5]. A. K. Mohan, M. R. Saranya and K. Anusudha, "Improved reversible data hiding using histogram shifting method," 2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kozhikode, 2015, pp. 1-5.

[6]. K. Mohan, M. R. Saranya and K. Anusudha, "An algorithm for enhanced image security with reversible data hiding," 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, 2014, pp. 1042-1045.

[7]. Q. Zhang, "Study on Image Encryption Algorithm Based on Chaotic Theory," 2013 International Conference on Information Science and Cloud Computing Companion, Guangzhou, 2013, pp. 635-639.

[8]. V. Ba´noci, G. Buga´r, D. Levicky´, Z. Klenovicˇova´, ”A Novel JPEG Stega- nography Method Based on Modulus Function with Histogram Analysis,” Radioengineering, 2012, vol. 21, no. 2, p. 758–763. ISSN: 1805-9600.

[9]. J. K. Saini, H. K. Verma, ”A Hybrid Approach for Image Security by Combining Encryption and Steganography”, Proc. of 2nd Intl. Conf. ICIIP 2013, Waknaghat (India), 2013, p. 607–611. ISBN: 978-14-6736- 101-9. DOI: 10.1109/ICIIP.2013.6707665.

[10]. R. Matthews, ”On the Derivation of a ’Chaotic’ Encryption Algo- rithm,” Cryptologia, 1989, vol. 8, no. 6 p. 29–41. ISSN: 0161–1194. DOI: 10.1080/0161-118991863745.

[11]. J. Fridrich, ”Symmetric Ciphers Based on Two-dimensional Chaotic Maps,” Intl. J. of Bifurcation and Chaos, 1998, vol. 8, no. 6, p. 1259– 1284. ISSN: 0218–1274. DOI: 10.1142/S021812749800098X.

[12]. F. J. S. Moreira, ”Chaotic dynamics of quadratic maps,” Master’s thesis, University of Porto (Portugal), 1992, 50 p.