DOI: 10.13140/RG.2.2.19539.58402

The Survey of Combination of Steganography and Cryptography in LSB and Encryption Techniques

Vishal Garg[1], Vanita Rani[2]
[1]*M.Tech (Scholar),* [2]*Assistant Professor*
Department of Computer Science Engineering, Indo Global College of Engineering, Chandigarh

Abstract - Steganography and Cryptography are well identified and widely used techniques that manipulate information in order to encryption or hide their being. These two techniques share the common goals and services of protecting the confidentiality, reliability and availability of info from unapproved access. In this paper, a data hiding system that is based on audio steganography and cryptography is planned to secure data transfer between the source and destination. Audio intermediate is recycled for the steganography and a LSB (Least Significant Bit) algorithm is employed to encode the message inside the audio file. The Study system was evaluated for effectiveness and the prior result shows that, the encryption and decryption approaches used for emerging the system make the security of the proposed system more efficient in securing data from illegal access. The system is consequently, suggested to be used by the Internet users for establishing a more secure communication.

Keywords - Steganography, cryptography, Least Significant Bit, Secure Data.

I. INTRODUCTION

Cryptography and Steganography are well identified and extensively used methods that manipulate information in order to cipher or hide their presence correspondingly. Cryptography challenges a message so it cannot be understood;[1] the Steganography hides the message so it cannot be seen. According to cryptography is not sufficient for secure communication. Even though both methods deliver security, a study is completed to association both Cryptography and Steganography methods into one system for better discretion and safety. Joining these two methods together for the purpose of developing a system that will advance the confidentiality and security of the communication is however, the goal of this research [2]. According to, the influence of steganography is in hiding the underground message by obscurity, hiding its existence in a non-secret file. In that intellect, steganography is dissimilar from cryptography, which involves making the content of the secret message incomprehensible while not avoiding non-intended [3] observers from learning about its existence. The success of steganography technique is contingent completely on the ability to hide the message such that an observer would not suspect its existence; the greatest exertion must go into confirming that the message is invisible unless one recognizes what to look for. The way in which this is done will change for the detailed media that are used to hide the info[4]. In each case, the value of a steganography method can be unhurried by how much information can be concealed in a carrier before it becomes obvious, each method can thus be assumed of in terms of its capacity for information hiding. Steganography, the talent of transmission information just between you and me, is appreciated by embedding secret messages into innocent cover matters such as numerical images, audios and videos. The very presence of the communication itself is hidden since the stego-object looks the same as the cover. However, as the cover object is inescapably changed, the covert communication can still be perceived by some numerical resources [5].

Steganography is a talent of hiding statement by embedding message into an innocuous observing cover media. Using steganography, an underground message is embedded inside a piece of credulous information and sent deprived of anyone knowing the survival of the secret message. Assurances can be hidden exclusive all sorts of cover information [6]:

- Text,
- Image,
- Audio,
- Video and so on.

Most steganography values hide information inside images [7], as it is comparatively easy to implement. People refer image steganography as the art and knowledge of invisible message, which is to secrete the very presence of hidden message in digital images. Some evidences have interested active investigates and plentiful journals in the field of image steganography. For instance, images can convey a large of information especially on the internet. Moreover, the non-stationary of images makes image steganography hard to break. Nowadays, ordinal image has become a significant channel to bear stego information.

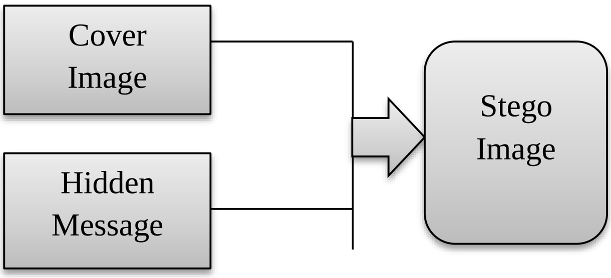

Fig.1: Simple scenario Steganography

DOI: 10.13140/RG.2.2.19539.58402

II. RELATED WORK

Bingwen Feng et.al, 2014 [10] described as, a binary image steganography scheme that aims to minimalize the embedding distortion on the texture is presented. They extracted the complement, alternation, and mirroring invariant local texture patterns from the binary image first. The weighted sum of crimp changes when flipping one pixel is then employed to measure the spinning alteration corresponding to that pixel. Vojtˇech Holub et.al,2014 [11] proposed a worldwide distortion design called worldwide wavelet qualified distortion that can be applied for entrenching in an arbitrary domain. The embedding distortion was computed as a sum of comparative variations of coefficients in a steering filter bank decomposition of the protection image. The directionality forces the embedding changes to such parts of the cover object that are problematic to model in multiple directions, such as traces or noisy regions, while avoiding smooth districts or clean edges. Saiful Islam et.al, 2014 [12] proposed a novel steganography method, where edges in the cover image have been used to surround messages. Amount of data to be embedded plays a significant role on the selection of edges, i.e., the more the quantity of data to be embedded, larger the use of weedier edges for embedding. Dr. Diwedi Samidha et.al,2013[13] in this purposed many steganography methods can be used like Least Significant Bit, layout organization schemes, substituting only l's or only zero's from subordinate nibble from the byte are measured for hiding secret message in an image. Along with these systems, some more methods were proposed, grounded on collection of random pixels from a duplicate and again secret data is hidden in accidental bits of these randomly designated pixels. Ge Huayong et.al,2011[14] reviewed steganography and steganalysis based on digital image. Perception and principle of steganography and steganalysis were demonstrated. Spatial domain and transform domain inserting methods are generalized. G. Prashanti et.al,2015,[15]In this paper, offers an analysis of recent realizations of LSB based spatial domain steganography that have an better steganography's ultimate objects, which are undetectable, robustness and capacity of hidden data. These methods can help researchers in empathetic about image steganography and numerous techniques of hiding data in an image. Laterally with this, two new methods are planned one for hiding secret message into cover image and the second is smacking a grey scale secret image into another grey scale image.

III. TECHNIQUES OF STEGANOGRAPHY

1. Data Hiding Method

Hiding the data, a username and password are compulsory prior to use the system. Once the user has been login into the system, the user can use the material (data) organized with the secret key to hide the data inside the preferred image [7]. This method is used to hiding the presence of a message by hiding information into several movers. This avoids the detection of hidden information.

2. Data Embedding Method

For recovering the data, a secret key is compulsory to recovering nether the data that have been fixed inside the image. Without the secret key, the data cannot be recovered from the image. This is to ensure the integrity and privacy of the data. The process of embedding the message inside the image, a secret key is desirable for recovering the message back from the image, the secret message that is removed from the system is transmission into text file and then the text file is crushed into the zip file and zip text file is translating it into the dualistic codes.

3. Data Extracting Method

It is used to recover an original message from the image; a secret key is needed for the confirmation. And for removing method, a secret key is desirable to check the key is accurate with interprets from the series of binary code. If key is matched, the process continues by forming the binary code to a closed text file, unzip the text file and allocation the secret communication from the text file to recover the original secret message.

IV. CRYPTOGRAPHY

Cryptography is an imperative component of any policy to address message broadcast security necessities. Cryptography is the study of approaches of sending messages in concealed form so that only the planned recipients can remove the cover and read the message. It is the applied art of changing messages or data into a dissimilar form, such that no-one can read them deprived of having access to the 'key'. The message may be transformed using a 'code' (in which case each character or group of types is substituted by an another one), or a 'cypher' or 'cipher' (in which case the message as a whole is transformed, rather than individual characters).Cryptology is the knowledge underlying cryptography. Cryptanalysis is the knowledge of 'breaking' or 'cracking' encryption arrangements, i.e. determining the decryption key. Cryptographic classifications are generically confidential along three autonomous dimensions:

1. Converting plain text to cipher text
2. Number of keys used [8].
    - Secret key
    - Public key
    - Digital signature and
    - Hash function.
3. Dispensation plain text.

V. COMBINED STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography must not be disordered with cryptography that contains transforming the message so as to make its denotation obscure to malicious people who

DOI: 10.13140/RG.2.2.19539.58402

intercept it. In this situation, the definition of contravention the system is different. In cryptography, the system is cracked when the attacker can read the secret message. Contravention a steganography system needs the attacker to distinguish that steganography has been used and able to read the embedded message[9]. Allowing to, steganography provides a resources of secret communication, which cannot be uninvolved without significantly changing the data in which it is embedded. In addition, the security of classical steganography system relies on privacy of the data encoding system. Once the encoding system is known, the steganography system is beaten. The figure below shows the mixture of cryptography and steganography:

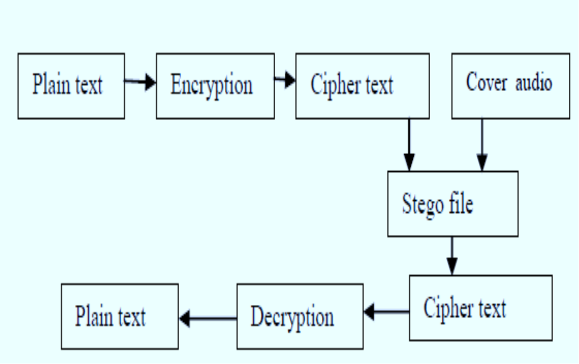

Fig.2 Combined Crypto and Stego.

However, it is always a good repetition to use Cryptography and Steganography composed for adding multiple layers of safety. By joining, the data encryption can be done by a software and then embed the cipher text in an audio or any additional media with the help of stego key. The grouping of these two approaches will enhance the security of the data embedded. This mutual chemistry will satisfy the necessities such as capacity, security and robustness for secure data transmission over an open channel.

VI. APPLICATIONS OF STEGANOGRAPHY

1. Secret Communications:-The use of steganography does not enunciate secret communication and therefore avoids existence of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can thus be transmitted without warning potential attackers.
2. Feature Tagging Essentials can be embedded classified an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also replicas all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
3. Copyright Protection: Copy protection mechanisms that prevent data, generally digital data, from being copied. The enclosure and analysis of water-marks to protect copyrighted material is answerable for the recent rise of interest in digital steganography and data embedding.

Table 1: Difference between Steganography and Cryptography

Title Name	Cryptography	Steganography
Objectives	Keeping the content of the message secret	Keeping the existence of the message secret
Applications	Used for information security	Used for information security
Security Services	• Confidentiality • Integrity • Non-repudiations • Authentication	• Confidentiality • Authentication
Problems	• Key distribution • Law enforcement	• Key distribution • Steganalysis

VII. CONCLUSION

In this paper, a system that collective the methods of cryptography and steganography to provide efficient method of hiding data from any unofficial users were offered. An audio medium was used for the steganography and the Least Significant Bit algorithm was working to encode the message inside the audio file. This proposed system does not tamper with the innovative size of the file even after encoding and also suitable for any type of audio file format. The encryption and decryption methods used with this organization make its security more robust. The system is therefore, recommended to use by Internet users for establishing a more secured communication.

VIII. REFERENCES

[1]. Deeply (Nov 2012) "Steganography With Data Integrity", International Journal Of Computational Engineering Research (ijceronline.com), Vol.2, Issue 7.

[2]. Attalla M. Al-Shatnawi(2012), "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, no. 79, 3907 – 3915.

[3]. T. Morel, J.H.P. Elf, M.S. Olivier, "An Overview Of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science ,University of Pretoria, 0002, Pretoria, South Africa.

DOI: 10.13140/RG.2.2.19539.58402

[4]. Prof. Akhil Khare, Meenu Kumar, J Palla Vi Khare(Oct 2010), "Efficient Algorithm For Digital Image Steganography", Journal Of Information, Knowledge And Research In Computer Science and Applications, ISSN: 0975 – 67281, Nov 09 to Oct 10, vol.1, Issue 1.

[5]. Sneak Aurora et al, Sanlam(Feb 2013), "A Proposed Method for Image Steganography Using Edge Detection", International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2).

[6]. Gabriel Hospodar, "Algorithms for Digital Image Steganography via Statistical Restoration"_ ESAT/SCD-COSIC and IBBT, Katholieke Universities Leuven Kasteelpark Ehrenberg 10, bus 2446, 3001 Heerlen, Belgium.

[7]. Shamim Ahmed Laskar and Kattamanchi Hemachandran(Dec 2012), "High Capacity Data Hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6.

[8]. Adel Almohammad, Robert M. Hierons "High Capacity Steganography Method Based Upon JPEG", The Third International Conference on Availability, Reliability and Security The JPEG standard uses 8x8 quantization tables.

[9]. Ross J. Anderson, Fabien A.P. Petitcolas(May 1998), "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481.

[10]. Feng, Bingwen, Wei Lu, and Wei Sun. "Secure binary image steganography based on minimizing the distortion on the texture." Information Forensics and Security, IEEE Transactions on 10.2 (2015): 243-255.

[11]. Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security 2014.1 (2014): 1-13.

[12]. Islam, Saiful, Mangat R. Modi, and Phalguni Gupta. "Edge-based image steganography." EURASIP Journal on Information Security 2014.1 (2014): 1-14.

[13]. Samidha, Diwedi, and Deepak Agrawal. "Random image steganography in spatial domain." Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on. IEEE, 2013.

[14]. Huayong, Ge, Huang Mingsheng, and Wang Qian. "Steganography and Steganalysis based on digital image." Image and Signal Processing (CISP), 2011 4th International Congress on. Vol. 1. IEEE, 2011.

[15]. Prashanti, G., and K. Sandhyarani. "A New Approach for Data Hiding with LSB Steganography." Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Springer International Publishing, 2015.