A Review on Secure Communication Method Based on Encryption and Steganography

Kinan Sharon Minz[1], Pradeep Singh Yadav[2]

[1,2]*Dept. of Communication, Shri Shankaracharya Technical Campus, SSGI, Durg, C.G., India*

Abstract: Steganographic techniques were subject to investigation of many authors and researchers. Some studies even investigate the possibility of using steganography for dangerous purposes. Internet fast expansion and digital multimedia formats allow many approaches for developing steganographic applications. Moreover, steganography can be used for other purposes than hiding information, such as implementation of network QoS services or providing better security of network packets. Accuracy of simulations can be improved by steganographic means. In practice, there are many steganographic methods that rely on a strong mathematical background (Discrete Cosine Transform, Wavelet Transform, temporal or frequency masking). Alternatively, there are other approaches that rely on modification of various characteristics of digital file formats such as: least significant bit, unused fields/bits from headers, compression ratio (in case of compressed multimedia files) and others. Although these techniques do not rely on a complicated theory and usually do not require a high amount of resources, they offer decent performance in what concerns information hiding vs. detection and identification rate. In paper the authors present an analysis of various steganographic algorithms. The authors focus on some qualitative aspects such as: complexity, hardware resources, processing needs, carrier's capacity for hiding information, deterioration of the carrier after embedding external information. In many cases, steganography is not strong enough to be used as soul method for hiding information. For these cases, steganography can be enhanced with a more or less complex form of encryption. This paper presents a combination between encryption based on a low resource consuming method and steganography.

Keywords: Data hiding; Text; Security; Steganography; Encryption; Communication

Proposed Methodology:

Steganography is done by LSB method. This paper, a novel data-hiding technique based on the LSB technique of digital images is presented. Data hiding is one of best topic in secret communication. A lossless data hiding technique using LSB in images is presented in this paper. LSB data hiding technique does not affect the visible properties of the image. Steganography is art and science of hiding the fact that communication is taking place. Secrets can be hidden in all types of medium: text, audio, video and images. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. This paper deals with hiding text in an image file using Least Significant Bit (LSB) technique. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image.

LSB Methods:

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

Block Diagram:

A message is embedded into the image by the stego system encoder. The resulting stego image is transmitted over a channel to the receiver. The stego system at the decoder end, using the same key or password, will decode the stego image. Block diagram is shown in figure below.

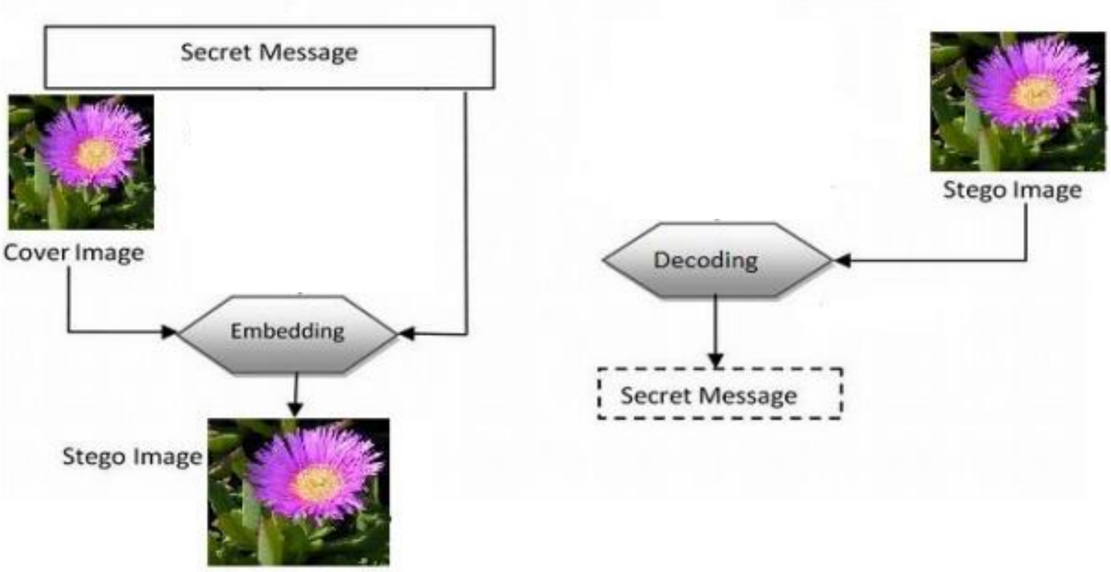
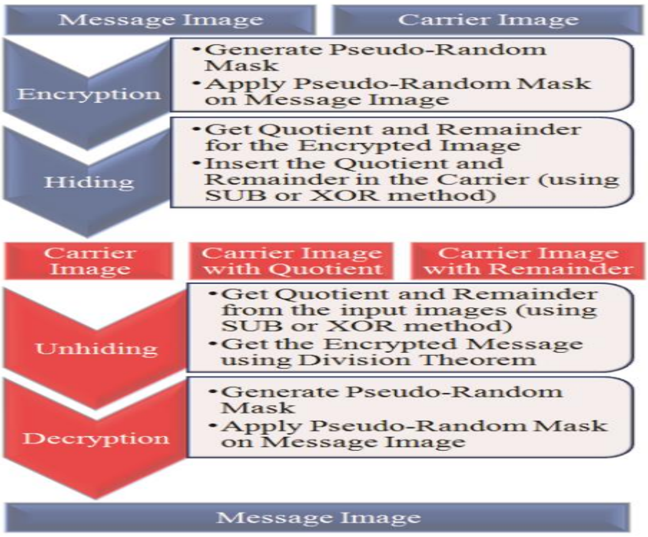


Figure: Block Diagram of Steganography

Flow Chart:


Message Image
Carrier Image
Encryption
•Generate Pseudo-Random Mask
•Apply Pseudo-Random Mask on Message Image
Hiding
•Get Quotient and Remainder for the Encrypted Image
•Insert the Quotient and Remainder in the Carrier (using SUB or XOR method)
Carrier Image
Carrier Image with Quotient
Carrier Image with Remainder
Unhiding
•Get Quotient and Remainder from the input images (using SUB or XOR method)
•Get the Encrypted Message using Division Theorem
Decryption
•Generate Pseudo-Random Mask
•Apply Pseudo-Random Mask on Message Image
Message Image

Literature Survey:

Shamim Ahmed Laskar and Kattamanchi Hemachandran (2012) proposed that with the spread of digital data around the world through the internet, the security of the data has raised a concern to the people. Many methods are coming up to protect the data from going into the hands of the unauthorized person. Steganography and cryptography are two different techniques for data security. The main purpose in cryptography is to make message concept unintelligible, while steganography aims to hide secret message. Digital images are excellent carriers of hidden information. We propose a method of combining steganography and cryptography for secret data communication. In this paper, authors propose a high performance JPEG steganography along with a substitution encryption methodology. The approach uses the discrete cosine transform (DCT) technique which used in the frequency domain for hiding encrypted data within image. Experimental results show that the visual and the statistical values of the image with encrypted data before the insertion are similar to the values after the insertion thus reduces the chance of the confidential message being detected and enables secret communication. The effectiveness of the proposed method has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).

Arun A.S. and George M. Joseph (2013) proposed a novel cryptographic technique that exploits the advantages of two important techniques steganography and chaotic image encryption. Steganography is the technique of hiding the message within a cover media. Once the message is embedded within the cover image, it is encrypted using triple key chaotic image encryption. So altogether this method provides a four layer security to the original message. Various analyses were done and the results of the experiments are very encouraging and in future, this method can be extended to support media other than images.

R.Poornima et al. (2013) presented that hiding Capacity plays a vital role for efficient covert communication. This is achieved by Steganography. Steganography is the science of hiding the information into the other information so that the hidden information appears to be nothing to the human eyes. There are many ways to hide information inside an image, audio/video, document etc. But Image Steganography has its own advantages and is most popular among the others. This paper gives a review of various methods such as image domain and transformation domain algorithms available for implementing Image Steganography. In this paper, a high capacity Image Steganography schemes are discussed for different file formats. Covert communication is taking place by encrypting the password for information to be protected. The intended receiver will decrypt the information using that password.

Apoorva Shrivastava and Lokesh Singh (2016) proposed that security in data communication is a very important concern today. It is used in almost every region like e-commerce, education, and industry and data warehouse. Securely sending and receiving data in the above area is an important as the data is crucial. Maintain the security become tough as the data inherent characteristics are also different. So the main focus of this paper is to study and discuss the trends which are already been proposed in the direction of cryptography and steganography. The gap identification have been provided by this study and based on the identification future suggestions have been provided.

Marwa E. Saleh et al. (2016) authors proposed that cryptography and steganography could be used to provide data security, each of them has a problem. Cryptography problem is that, the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. Steganography problem is that once the presence of hidden information is revealed or even suspected, the message is become known. According to the work in this paper, a merged technique for data security has been proposed using Cryptography and Steganography techniques to improve the security of the information. Firstly, the Advanced Encryption Standard (AES) algorithm has been modified and used to encrypt the secret message. Secondly, the encrypted message has been hidden using method in . Therefore, two levels of security have been provided using the proposedhybrid technique. In addition, the proposed technique provides high embedding capacity and high quality stego images.

R. Rejani et al. (2016) proposed that in today's digital world applications from a computer or a mobile device consistently used to get every kind of work done for professional as well as entertainment purpose. However, one of the major issue that a software publisher will face is the issue of piracy. Throughout the last couple of decades, almost all-major or minor software has been pirated and freely circulated across the internet. The impact of the rampant software piracy has been huge and runs into billions of dollars every year. For an independent developer or a programmer, the impact of piracy will be huge. Huge companies that make specialized software often employ complex hardware methods such as usage of dongles to avoid software piracy. However, this is not possible to do for a normal independent programmer of a small company. As part of the research, a new method of software protection that does not need proprietary hardware and other complex methods are proposed in this paper. This method uses a combination of inbuilt hardware features as well as steganography and encryption to protect the software against piracy. The properties or methods used include uniqueness of hardware, steganography, strong encryption like AES and geographic location. To avoid hacking the proposed framework also makes use of self-checks in a random manner. The process is quite simple to implement for any developer and is usable on both traditional PCs as well as mobile environments.

Ramadhan Mstafa et al. (2016) proposed that innovation of technology and having fast Internet make information to distribute over the world easily and economically. This is made people to worry about their privacy and works. Steganography is a technique that prevents unauthorized users to have access to the important data. The steganography and digital watermarking provide methods that users can hide and mix their information within other information that make them difficult to recognize by attackers. In this paper, we review some techniques of steganography and digital watermarking in both spatial and frequency domains. Also we explain types of host documents and we focused on types of images.

Dipti Kapoor Sarmah and Neha Bajpai (2017) proposed that steganography and cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations like DCT, FFT and Wavelets etc. In this project we are developing a system where we develop a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module. In Cryptography we are using AES algorithm to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured.

Marwan Ali Albahar et al. (2017) proposed that there are two solutions in data security field for ensuring that only legitimate recipients will have access to the intended data: Steganography and cryptography. These solutions can be used for providing a high level of security. With the exponential growth of challenges in the field of computer security, the use of Bluetooth technology is expanding rapidly to expose many of these challenges on the surface. One of these challenges is the MITM attack during Bluetooth pairing process. In this paper, we will steer the wheel to concoct a novel method based on Steganography to fortify the pairing process and thwart MITM attacks. In the light of this study, a thorough experiment will be conducted based on the proposed method. Moreover, we will provide results of the experiment in order to show the applicability of our novel method. Furthermore, we will sketch some new ideas that will be used in our future research work.

Rashmi A. Sonawane et al. (2017) proposed that a texture synthesis process resample a smaller texture image, which synthesizes a new texture image with a similar local appearance and an arbitrary size. the texture synthesis process into Steganographic to conceal secret messages. In contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of texture synthesis. This allows us to extract the secret messages and source texture from a Stego synthetic texture. This approach offers three distinct advantages. First, scheme offers the embedding capacity that is proportional to the size of the Stego texture image. Second, a Steganalytic algorithm is not likely to defeat our Steganographic approach. Third, the reversible capability inherited from our scheme provides functionality, which allows recovery of the source texture. algorithm can provide various numbers of embedding capacities, produce a visually plausible texture images, and recover the source texture.

Ştefan MOCANU et al. (2017) proposed that for some people a science, for other people just an art, steganography is in fact an ancient method of embedding a message into an apparently uninteresting carrier. Aiming to protect information, steganography is considered to be a close relative of encryption although they have different approaches. While encryption scrambles the message based on a certain algorithm so it can't be understood by anyone that does not hold the unscrambling key, steganography works on hiding the message without the need to deteriorate it. Minor alteration of the carrier file is accepted since steganography does not affect its useful content. Actually, steganography exploits file redundancy, file headers or, in case of multimedia content, replaces information that can't be used or perceived by the human eyes or ears. In this paper, a combination of image based steganography with encryption is presented. The encryption and decryption are based on two different files in which, by steganographic means, important information is hidden. The original message (the secret message) can be restored only if both files arrive safe at destination. There are no constraints regarding the image file types. The most important contribution resides in how the original information is encrypted and embedded into different graphic files, sent to the destination through different channels and then restored. Comparative performance tests were performed.

Radu Nicolae et al. (2018) proposed that current and upcoming weather forecasts play a very important role in our society, from big companies to each simple individual that wants to be prepared and adapt to any changes. Many entities use data provided by each country's National Weather Service in order to combat any negative impact the conditions may have on their daily activities. Unfortunately, the service does not provide a very accurate set of parameters, instead it gives an average forecast for a given area of interest. Here is where personal weather stations come to the rescue. Not only they are cheap and easy to set up, but they also provide the user with the exact data he wants. Depending on each individual's needs, the weather station can be adjusted and equipped with a wide range of sensors, ranging from wind speed and UV radiation to air quality sensor. Using an Arduino development board (or equivalent) that is available on a large scale, the integration of the sensors can be done without many challenges and, if the user does want to implement this feature, the acquired data can be uploaded and used on the internet. Being supported by a very large community, Arduino boards can implement these features without implying a big money or time penalty. One of the most important aspects a weather station brings, apart from the possibility to build it at a very low price, is that the user can have access to any weather data that defines his area of interest, thus increasing the accuracy and the resolution of the forecast and allows early warning in case of extreme weather phenomena.

Expected Outcome: The encrypted data will be properly decrypted at the receiver side by using the LSB method.

Conclusion: Steganography is a technique of covering the data in such a way that the message could be transmitted secretly and only the sender and receiver knows the way of decrypting that secret text or message. Steganography increases the security of data to be transmitted and also ensures that only authorized personnel can have access to that message. This paper presents a review of steganography and techniques that are used for steganography. Various papers have been reviewed on steganography. It is studied that there is various types of steganography like text, audio, video, image, network or protocol steganography [7]. This shows that text or data using steganography can be hidden in many ways. Techniques of steganography have been reviewed and studied in the paper.

Reference:

1) Arun A.S. and George M. Joseph , "High Security Cryptographic Technique Using Steganography And Chaotic Image Encryption", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 12, Issue 5, Jul. Aug. 2013.
2) Dipti Kapoor Sarmah and Neha Bajpai, "Proposed System for data hiding using Cryptography and Steganography"
3) Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, Issue No. 6, 2016
4) Radu Nicolae PIETRARU, Alexandru-Ștefan BANU, Ștefan MOCANU, Daniela SARU, "Low Cost Technologies for Awarness and Early Warning in Conditions of Severe Weather" , The 14th International Scientific Conference eLearning and Software for Education Bucharest, April 19-20, 2018 10.12753/2066-026X-18-118
5) Shamim Ahmed Laskar and Kattamanchi Hemachandran, "SECURE DATATRANSMISSIONUSING STEGANOGRAPHY AND ENCRYPTION TECHNIQUE", International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.
6) Abboud, G., Marean, J. & Yampolskiy, R. (2010). Steganography and Visual Cryptography, In Computer Forensics, IEEE Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 25-32. 2. Djebbar, F.,
7) Ayad, B.& Meraim, K. (2012). Comparative study of digital audio steganography techniques, EURASIP Journal on audio, speech and music processing, 2012(1), pp. 1-16.
8) . Doshi, R., Jain, P. & Gupta, L. (2012). Steganography and Its Applications in Security, International Journal of Modern Engineering Research, 2(6), pp. 4634-4638.
9) Elminaam, D., Kader, H. & Hadhoud, M. (2009). Performance Evaluation of Symmetric Encryption Algorithms, Communications of the IBIMA, 8pp. 58-64. 5. Gleason, N. (1987). Fun with codes and ciphers workbook, Dover Publications Inc. 6.
10) Iordache, D., Pribeanu, C., & Balog, A. (2012). Influence of Specific AR Capabilities on the Learning Effectiveness and Efficiency, Studies in Informatics and Control, 21(3), pp. 233-240.
11) Jayaram, P., Ranganatha, H., Anupama, H. (2011). Information hiding using audio steganography – a survey, International Journal of Multimedia & Its Applications (IJMA), 3(3), pp. 86-96.
12). Mazurczyk, W. & Kotulski, Z. (2006). New security and control protocol for VoIP based on steganography and digital watermarking, Annales UMCS, sectio AI – Informatica, 5, pp. 417-426.
13) 9. Mazurczyk, W., Wendzel, S., Villares, I. & Szczypiorski, K. (2016). On importance of steganographic cost for network steganography, Security and Communication Networks, 9(8), pp. 781–790.
14) Mona, M., Chitra, S., Gayathri, V. (2014). A survey on various encryption and decryption algorithms, Singapore Journal of Scientific Research, 6(6), pp. 289-300.
15) Nissar, A. & Mir, A. (2010). Classification of steganalysis techniques: A study, Journal of Digital Signal Processing, 20(6), pp. 1758-1770. 12. Saeed, M. (2013). A new technique based on chaotic steganography and encryption text in DCT domain for color image, Journal of Engineering Science and Technology, 8(5), pp.508–520. 1
16) Saha, B. & Sharma, S. (2012). Steganographic Techniques of Data Hiding using Digital Images, Defence Science Journal, 62(1), pp.11-18.
17) Saleh, S. (2013). A secure data communication system using cryptography and steganography, International Journal of

Computer Networks & Communications (IJCNC), 5(3), pp.125-137.

18) Singh, S. & Attri, V. (2015). State-of-theart Review on Steganographic Techniques, International Journal of Signal Processing, Image Processing and Pattern Recognition, 8(7), pp.161-170.

19) Subhedar, M. & Mankar, V. (2014). Current status and key issues in image steganography: A survey, Computer Science Review, 13–14, pp.95–113.

20). Thangadurai, K. & Devi, G. (2014). An analysis of LSB based image steganography techniques, In IEEEInternational Conference on Computer Communication and Informatics, pp.1-6.

21) Tripathi, R. & Agrawal, S. (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques, International Journal of Advance Studies in Informatics and Control, Vol. 26, No. 1, March 2017 http://www.sic.ici.ro 125 Foundation and Research in Computer, 1(6), pp.68-76.

22) Tseng, H. & Leng, H. (2013). A Steganographic Method Based on PixelValue Differencing and the Perfect Square Number, Journal of Applied Mathematics, 2013, ID 189706, online.

23) Wang, K., Lu, Z. & Hu, Y. (2013). A high capacity lossless data hiding scheme for JPEG images, Journal of Systems and Software, 86(7), pp.1965-1975.

24) Warkentin, M., Bekkering, E. & Schmidt, M. (2008). Steganography: Forensic, Security, and Legal Issues, Journal of Digital Forensics, Security and Law, 3(2), article 2, online.

25). Wendzel, S., Mazurczyk, W., Caviglione, L. & Meier, M. (2014). Hidden and Uncontrolled - On the Emergence of Network Steganographic Threats, In Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe Conference, pp. 1-11. 23. Zhang, J., Cox, I. & Doerr, G. (2007). Steganalysis for LSB Matching in Images with High-frequency Noise,In IEEE 9th Workshop on Multimedia Signal Processing, pp. 385-388