IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 6, June 2016

Information Security Using Cryptography and Steganography

Hareendran Ullattil

Lecturer in Electronics Engineering, Government Polytechnic College, Meenangadi, Wayanad, Kerala.

Abstract: In today's information technology, the internet is an essential part for communication and information sharing. Providing confidential information and establishing concealed association has been a great interest since long time ago. The security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. Cryptography and steganography are the two popular methods available to provide security. Cryptography scrambles a message so it cannot be understood and generates cipher text. Steganography word is derived from Greek, literally means "Covered Writing". Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. It includes vast ways of secret communications methods that conceal the message's existence. In Cryptography, the meaning of data has been changed. So, it makes intention to the hacker to hack or destroy the data. In our proposed paper, we implement a method by integrating both Cryptography and Steganography for information security. It not only changes the meaning of data but also hides the presence of data from the hackers. In order to secure the transmission of data, Steganography has to be implemented that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is intended recipient.

Keywords: Cryptography, Steganography, LSB, Data hiding, Stego-image, Diffie-Hellman Key Exchange

I. INTRODUCTION

Information security has grown as a significant issue in our digital life. The development of new transmission technologies forces a specific strategy of security mechanisms especially in state of the data communication. The significance of network security is increased day by day as the size of data being transferred across the Internet. Cryptography and steganography provide most significant techniques for information security.[1]

The most important motive for the attacker to benefit from intrusion is the value of the confidential data he or she can obtain by attacking the system. Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks. A solution for this issue is using the advantage of cryptography and steganography combined in one system.[2]

Cryptography is the science of using mathematics to encrypt and decrypt data to keep messages secured by transforming intelligible data form (plaintext) into unintelligible form (ciphertext). The term cryptography has come from the Greek word "kryptós" standing for "hidden" and "gràphin" standing for "writing". Thus, the proper meaning of cryptography is "hidden writing". Any cryptosystem consists of plaintext, encryption algorithm, decryption algorithm, Cipher text, and Key.

Plaintext is message or data which are in their normal, readable (not encrypted) form. Encryption is the process of converting plaintext to cipher text by using key. Cipher text results from encryption by applying the encryption key on the plaintext. Decryption is the process of retrieving the plaintext back from the cipher text. The Key is used info to control the cryptosystem (cipher system), and it is known by the sender and receiver only. While cryptography is very powerful for securing data; the cryptanalysts could success to break the ciphers by analyzing the contents of cipher text to get back the plaintext. [3-4]

The two main branches of cryptography are cryptanalysis and cryptology. Cryptanalysis refers to applying different method so as to break into a system or cipher text without having the knowledge of the key. This is also referred to as breaking the cryptosystem.

Below are the four parts of all cryptographic process:

Plaintext: Clear text or unscrambled text to be sent to another person or entity over the network. It could be a simple text document, personal information, a simple text document to be transmitted over the network.

Cipher text: Cipher text refers to information that have been scrambled and difficult to understand by others unless with the knowledge of the correct key e.g. encrypted text to be transmitted over the network.

Key: This refers to formula, mathematical value or process that can be used to encode or decode a message. Keys are used to convert messages or information to a cipher text. [5]

Cryptographic Algorithm: This could take a form of formula which can be used to encrypt or scramble a plain message into a form that cannot be easily understood by anybody unless with the knowledge of the key.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 6, June 2016

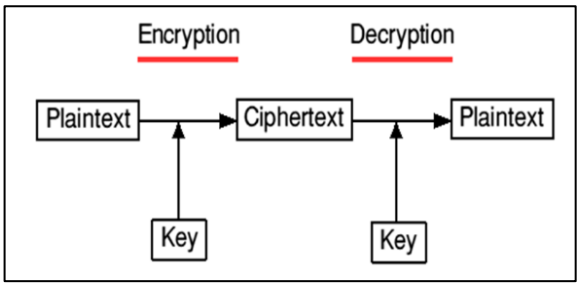


Figure 1: Basic concept of cryptograph

Steganography:

Steganography is the science of writing hidden messages to guarantee information which is accessible only by authorized parties. It is the practice of hiding information usually text messages, inside other files (host files). The practice of hiding information is called stego. Information can be hidden or embedded inside any type of multimedia files especially image files. The host files can then be exchanged over an insecure medium without anyone knowing what really lies inside them. Therefore, steganography in contrast with cryptography, where the existence of the message is clear, but the meaning is obscured. Steganography applications conceal information in other, seemingly innocent media. Steganographic results may masquerade as other file for data types, be concealed within various media, or even hidden in network traffic or disk space. Information hiding techniques provide an interesting challenge for digital forensic investigations. Information can easily traverse through firewalls undetected.[6]

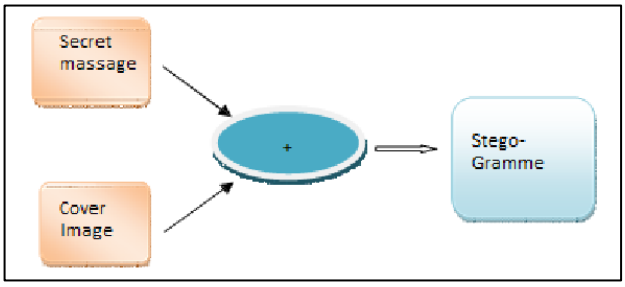


Figure 2: Steganographic system

The steganography approaches can be divided into three types.

Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

Secret Key steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

Public Key Steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

Combined Crypto-Steganography:

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. [7]

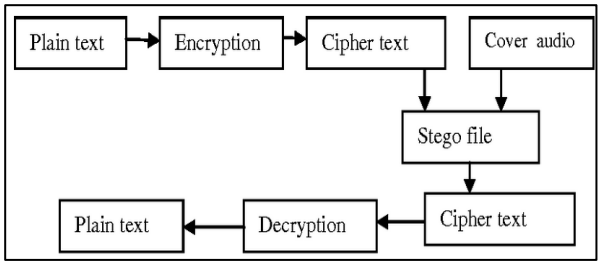


Figure 3: Combination of Crypto-Steganography

This combined chemistry will satisfy the In figure 3, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message.

The proposed method describes two steps for hiding the secret information by using the public steganography based on matching method in different regions of an image.

The First step is converting the Plain text message into cipher text using Public-key Encryption algorithm requirements such as capacity, security and robustness for secure data transmission over an open channel. A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 4.

The next step is to find the shared stego-key between the two communication parties (SENDER and RECIPIENT) over insecure networks by applying Diffie-Hellman Key exchange protocol. At the end the protocol, each side recovers his/her received public key to reach the shared values between them, that's mean SENDER & RECIPIENT have arrived same sego-key value. [8]

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 6, June 2016

II. OBJECTIVES

1. To improves communication security and reliability by encrypting the initial message.
2. To study of combination of Cryptography and Steganography.
3. To comparison between the resulting stego images and their histograms with cover images and their histograms.

III. REVIEW OF LITERATURE

Cryptography is the art of hiding information by encryption and decoding it by decryption. Cryptography provides integrity, authentication, and maintain the secrecy of information. Steganography in Greek means "covered writing". Steganography is the art of concealing the existence of information within seemingly innocuous carriers. information security is gaining more attention due to the increase in the size of data being transferred over the Internet. One of the proposed solutions is the exploitation of the advantages of cryptographic and steganographic techniques through their combination into a hybrid technique.

[B. Padmavathi and S. R. Kumari], authors conducted a performance analysis survey on various algorithms like DES, AES, RSA combining with LSB substitution technique which serves well to draw conclusions on the three encryption techniques based on their performances in any application. It has been concluded from their work that AES encryption is better than other techniques as it accounts for less encryption, decryption times and uses less buffer space.[9]

[R. Das and T. Tuithung], authors performed a modern method in which use Huffman encoding to hide data. They took a grey level image of size m*n as cover image and p*q as a secret image. After that, they executed the Huffman encoding over the secret image and every bit of Huffman code of a secret image is hidden into a cover image utilizing LSB algorithm.[10]

[S. E. Thomas, S. T. Philip, S. Nazar, A. Mathew, and N. Joseph], the authors encrypted the secret data by use AES algorithm and hashed the key using SHA-1 to prevent from attacks. After that, they used the LSB technique to embed the encrypted information in image, video or audio. The receiver must implement the key which is hashed in sender side. The secret data can be hidden in any type of media which affords more security.[11]

Zhou., et al.in, "Research and implementation of RSA algorithm for encryption and decryption", Proposed an RSA algorithm for the secure transmission of data. To increase the efficiency symmetric key algorithms and public-key cryptography algorithms are combined together. Symmetric key cryptosystem is used to encrypt the confidential information which is needed to be sent while RSA asymmetric key cryptosystem is used to send the DES key. This takes advantage of both the two kinds of cryptography, namely, high-speed DES and RSA key management mechanism. [12]

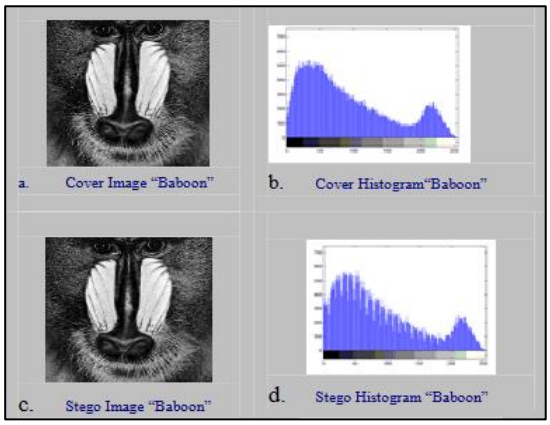
IV. RESEARCH METHODOLOGY

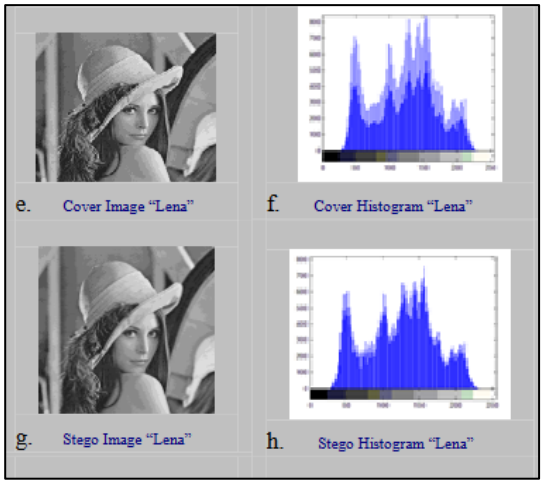
Steganography and cryptography are very important techniques used in data security to hide and secure secret messages in transmitted data. This paper will introduce, implement and test a novel methodology which can be used as a secure and highly efficient method of data hiding and data extracting. Some efficiency parameters will be experimentally obtained and compared with other existing methods parameters to prove the efficiency of the proposed methodology.

Books, educational and development journals, government papers, and print and online reference resources were only some of the secondary sources we used to learn about the composition, use, and impacts of data security using cryptography and steganography.

V. RESULT AND DISCUSSION

the change in histograms is influenced by the properties of image (i.e. the smooth area and edge area), so the larger number of edge areas in the original image, the more change in histogram of stego-image such as Baboon and Lena contrast to Pepper image. This is because the method that is used in hiding in smooth areas is MPK_PVD method.





IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 6, June 2016

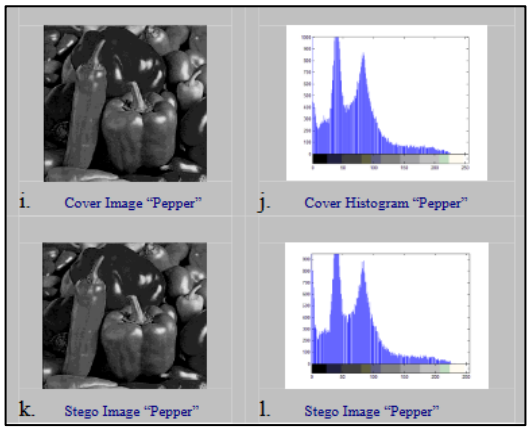


Figure 4: Three cover images and output stego-images used in system simulation with their corresponding histogram

In figure 4, a comparison between the resulting stego images and their histograms with cover images and their histograms has been made. We can see that there is no significant change in stego histograms and visual quality of the resulting stego-image of the three images.[13]
In table 1, a comparison between the proposed merged method has been made by hiding (18.6113.003, and 16.394) secret bytes in 256 x256 cover images (Baboon, Lena, and Peppers) respectively.

Table 1: comparison the Algorithm with the Proposed Algorithm

Cover Image 256*256	Hiding Capacity (bytes)	PSNR of Method in [21]	Hiding Capacity (bytes)	PSNR of Proposed Method
Baboon	18.616	33.80	18.624	41.7875
Lena	13.003	43.56	13.008	44.9864
Pepper	16.394	36.91	16.400	43.6845

The results indicate that, the proposed method has higher PSNR values and also the PSNR values are much greater than 36 dB. This proves the suitability of the proposed method.[14]

VI. CONCLUSION

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. The present study is designed to combine the features of both cryptography and steganography, which will provide a higher level of security. It is better than the technique used separately. Simple LSB method was used to embed the secret message into the image. The LSB in each selected pixel can be used to conceal the message binary code. It is also found that combination of cryptography and steganography enhance the security and reliability of message as first message is encrypted and using steganography hide it to other carrier like digital image, video file or any other.

REFERENCES

[1] M. H. Rajyaguru, "Crystography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.
[2] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975–8887) Volume, 2010.
[3] K. R. Babu et al, "A Survey on Cryptography and Steganography Methods for Information Security," International Journal of Computer Applications (0975 – 8887), Vol. 12, No.2, PP. 13-17, November 2010
[4] B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithm, and Source Code in C (cloth)," pp. 1–1027, January 1996.
[5] A. Monika, and M. Pradeep, "A comparative survey on symmetric key encryption techniques", International journal on computer science and engineering," 2012, vol. 4, issue 5, pp.877-882.
[6] Domenico Bloisi and Luca Iocchi, "Image Based Steganography and Cryptography", Sapienza University of Rome, Italy.
[7]Bharti,P.,and Soni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,International Journal of Computer Applications,Vol.58,No.18,2012,pp1-5
[8] Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, "A Survey on Cryptography and Steganography Methods for Information Security", Internaltional Journal of Computer Applications(0975-8887), Volume 12 – No. 2, November 2010.
[9] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution," IJSR, India, 2013.
[10] R. Das and T. Tuithung, "A novel steganography method for image based on huffman encoding," in Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on. IEEE, 2012, pp. 14–18
[11] S. E. Thomas, S. T. Philip, S. Nazar, A. Mathew, and N. Joseph, "Advanced cryptographic steganography using multimedia files," in International Conference on Electrical Engineering and Computer Science (ICEECS-2012), 2012.
[12] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." Proceedings of 2011 6th international forum on strategic technology. Vol. 2. IEEE, 2011.
[13] R.O. El Safy, H. H. Zayed, and A. El Dessouki, "An adaptive steganography technique based on integer wavelet transform," ICNMInternational Conference on Networking and Media Convergence, PP.111-117, (2009).
[14] H.B. Kekre, P. Halarnkar, and K. Dhamejani, "Capacity Increase for Information Hiding Using Maximum Edged Pixel Value Differencing," Springer-Verlag Berlin Heidelberg , PP. 190-194, 2011.