International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

Improved Security In Steganography By Amalgaming Cryptography And Quick Response Code

Suseendran Surendran[1], Ramya Palaniappan[2], Nagaraj V[3]

[1,2]Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India
[3]Assistant Professor, Department of Electronics and Communication Engineering Knowledge Institute of Technology, Salem, Tamil Nadu, India

E-mail: [1]suseendrans@bitsathy.ac.in, [2]ramyanp@bitsathy.ac.in, [3]nagarajphd16@gmail.com

Abstract. Steganography and steganalysis established a greater pact of consideration from communication services and law practices. Many powerful and secure approaches of steganography and steganalysis have been developed with the advent of technology. Combat between steganography and steganalysis has become a significant topic to be handled in information security. Steganalysis is an efficient technique used to hide any encrypted data behind an image or any other digital media to make them more secure. This image can be converted into a Quick Response Code which can make the encryption more powerful. It can be said as a amalgamation of steganography and cryptography techniques into a single technique. The steganography can preserve the secrecy whereas the cryptography can prevent intrusion. The steganalysis can prevent intrusion and make data secure by maintaining the secrecy of data. This can be the solution to ensure the security of the data as it is concerned by implementing the steganography technique for images with the improvement on both image security & quality. This technique can prevent the data and media from the vulnerable attacks and other several threats. It uses more secure algorithms which are unbreakable when compared to its previous techniques.

Keywords Data hiding, Steganography, Steganalysis, Signature steganalysis, Statistical steganalysis, Stego-image, LSB

1. INTRODUCTION

In today's world, communication is the elementary need for most of the jobs. Almost all people like to transmit various types of messages with secrecy and like to ensure that their data is secure from hackers. All reside on Internet for data transmission which is not secure beyond a certain level. In order to transmit messages in a concealed way, two important approaches can be used. They are 1. Cryptography 2. Steganography. Cryptography enciphers the plain data into unreadable form known as cipher text making use of encryption key which is shared secretly between the sender and the receiver over the transmission medium. However, the transmission of encrypted message will arouse the suspicion of the hacker, who can further proceed with the process of silent eavesdropping, attacking and decrypting the message which violates the security of the transmitted message[3][4]. To overcome this defect, steganography can be followed. Steganography precisely means

"Covered writing" is an art of secret communication. To increase the security of message both cryptography and steganography can be amalgamated[5]. Steganalysis is the process of sensing the secreted messages entrenched in digital media which includes audio, video or text files being transmitted using steganography, it is analogous to cryptanalysis applied in cryptography.

2. STEGANOGRAPHIC METHODS

Steganography precisely means "Covered writing" is an art of secret communication. It involves various methods to hide the information within any multimedia content like audio, video or image files during transmission which will obscure the presence of communication. This process is referred to as "Embedding writing"[6]. The Internet provides progressively a broad medium of communication through which lots and lots of information is made available to the public. Such information being transmitted over the internet may include data in different formats such as text data, images, and audio files for mass communication [1].

An initial method to hide information was made for text data where imperceptible inks were used to conceal the data. Numerous methods are available for hiding images to ensure security and secrecy. These methods include various techniques such as inclusion of noise to the data being transmitted, appending Least Significant Bit (LSB) to the data to change its pattern, manipulation of images by applying various filters, using compression algorithms to reduce the capacity of data for effective transmission and modify some image properties such as luminance, pixels to make it unpredictable[12][13].

Commonly used method of hiding information in images involves making use of algorithm and coefficients of image to perform concealing of information[7][8]. These approaches hide information behind significant areas of cover image which makes them more robust to attacks. For audio files, steganography can be achieved by introducing small echoes to the carrier signals or add high amplitude signals to subtle carrier waves to mask them for better security.

Alternative method of hiding data in file system is to create a concealed partition for the files before being transmitted. These partitions are not visible when the file is transmitted typically. The user will not be aware of the hidden partition and cannot view the contents of the file. If the user is provided the name of the file and its associated password, then privilege is granted for the user to access the file. If not, there will not be any indication of file transmission over the medium[9]. of the file exists in the system. The ease and choice of use and availability of various steganographic tools involves law prosecution associated with transmission of illegitimate information via web page images, audio, and other type of files being communicated over the Internet. Techniques for information recognition being covered using steganographic approaches are needed using current technology.[1]

3. STEGANALYSIS

Steganalysis is the process of a steganography procedures for which the detection, extraction, destruction and manipulation of the secreted data in a stego-object[10]. Steganalysis finds its use in various domains such as computer forensics, cyber warfare, following the criminal events over the internet[11].

Steganalysis can be of numerous types for instance, some analysis merely spot the presence of secreted data, some attempt to detect and extract the concealed data, some just try to delete the secret message which some try without extracting the secret message and add some other kind of data to find the location where the data is secretly kept .There are various approaches for steganalysis which can be approximately categorized into two groups: Signature steganalysis and Statistical Steganalysis. The separation is built on whether the signature of the steganography approach and tool or the statistics of image is used to recognize the usage of steganographic tool or presence of hidden messages in images entrenched by steganography.

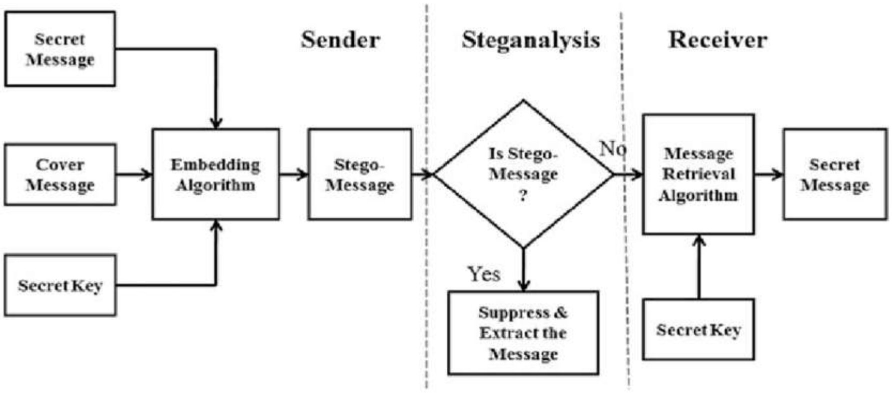

Fig. 1. Image Steganalysis

3.1 Statistical Steganalysis

When secret data is out of sight in an appearance, the statistics of the doppelgänger would have undergone alteration due to steganography approach used. Analysing this information i.e., statistics of image will help to detect the hidden information in the image. It can also be further divided into specific and universal statistical steganalysis[14][15]. Specific statistical steganalysis includes the statistical steganalysis techniques that utilizes a specific steganography embedding procedure or its slight variation: LSB embedding, LSB matching, JPEG compression. etc., The Universal statistical steganalysis includes the techniques that are not used for a specific steganography embedding technique. The concept here is to discover out proper delicate statistical measures with remarkable skills. A Neural network, clustering algorithms and other lenient figuring gears are then used to design the revealing exemplary from the trial data.[2]

3.2 Signature Steganalysis

The patterns and characteristics of steganographic technique act as signatures which can be used to recognize the concealed information in the image being transmitted[16]. It can also be further divided into Specific signature steganalysis and universal signature steganalysis.

The signature specific for every steganographic tool automatically provide information about steganographic approach used. For e.g. Jpegx, a data addition steganography bench, supplements the clandestine communication at the culmination of JPEG files sign and enhances a static monogram of the program before the clandestine communication before transmitting it. e. The moniker is the succeeding hex code: 5B 3B 31 53 00. The occurrence of this sign spontaneously infers that the image holds a clandestine note entrenched in essence via Jpegx. Common Sign steganalysis is not connected to specific steganographic gizmo. This is used entirely.

4 PROPOSED APPROACH

Our approach is described by the following five subsections which described the method of securing the message using steganography along with cryptography during transmission to protect them against steganalysis.

a. Encryption Algorithm

The encryption is a part of cryptography which is applied in steganalysis. This can protect the files of the user with a specific key which serves as a purpose of security. The files which are to be protected are obtained from the user. The files which are obtained from the user are encrypted using rijndael algorithm and it results in the generation of the key as a result of the encryption. This key can be used as a part of decryption and also in the retrieval of image from the QR code.

b. Hiding the Key

The steganography is the process of hiding any form of content behind a digital media. This is applied after cryptography in steganalysis. The key is a form of data which can be hidden behind any digital media like image. This is the part where the steganography and cryptography are combined.

The key which is obtained after the encryption of the image is hidden behind an image. The image into which the key should be hidden can be chosen by the user them self. This concept of hiding the key generated after the encryption of the selected file behind an image involves steganography.

c. Image to QR Conversion

The "stego-image" which has the shared key embedded within it is converted into a QR code for easy access and enhanced security. This helps the user to protect their data in a more secure way and QR code can be scanned easily. The reverse process of converting the QR into an image will result in decryption. The conversion of image to a QR code is carried out in order to ensure the ease of access and portability. The QR code can be easily applied or scanned from any hand-held device. This ensures the security as the decryption only happens when the key is known by the user.

d. Extraction of key from Image

The resulting QR can be scanned to view the image from which the key can be extracted. The key should be extracted from the image by scanning the QR code and this process of extraction is termed as "De-steganography". This key can be used to decrypt the file and view the original contents of the file.

The extraction of key is done to retrieve the file that has been hidden behind the image. This is the reverse process of those initial key generation processes.

e. Decryption

The decryption process is the counterpart of the encryption procedure applied. This method must be carried out in order to retrieve the original file which is encrypted and hidden. This helps the user to view their original file if the key is known. The decryption is the part of cryptography which is applied in steganalysis in order to enhance the security of the content provided. The decryption can be done only by the user who knows the key.

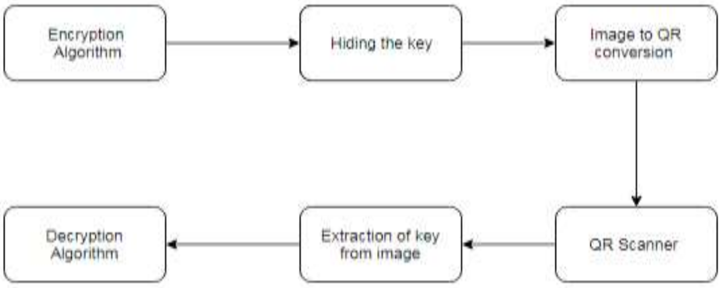

Fig. 2. Extracting the image on Amalgaming Steganography with QR Code

5. PERFORMANCE SPECIFICATION

While studying and designing steganographic systems certain related topics need to be concentrated more. It includes but not restricted to security (detectability of data), robustness and secrecy (struggle in extraction of hidden data). The relationship among them can be articulated by the steganographic triangle, which is shown in Fig.2. To progress one criterion, one has to compromise one or both of the other two criteria as all the three are inter-dependent.

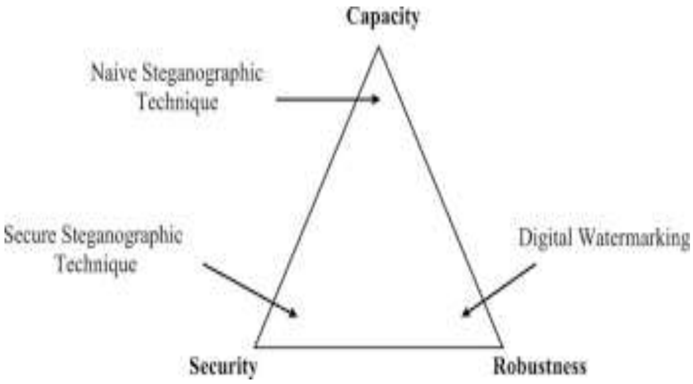
Capacity
Naive Steganographic Technique
Secure Steganographic Technique
Digital Watermarking
Security
Robustness

Fig. 3. Magic triangle – Steganography

Robustness refers to the ability of embedded message to withstand attack by distrustful third party or random addition of noise during the period of transmission of digital data over the transmission medium. Capacity refers to the upper bound on maximum number of bits that can be entrenched in the image while maintaining the file stego-image unpredictable. Security is the facility of the embedding carrier to be transmitted safely without any suspicion and remain undiscovered.

The steganography can preserve the secrecy whereas the cryptography can prevent intrusion. The steganalysis can prevent intrusion and make data secure by maintaining the secrecy of data. This can be the solution to ensure the security of the data as it is concerned by implementing the steganography technique for images with the This technique can prevent the data and media from the vulnerable attacks and other several threats. It uses more secure algorithm which are unbreakable when compared to its previous techniques. The metric-Peak signal to noise ratio (PSNR) is calculated for the proposed method is measured and found to be better than the existing methods as depicted in Fig. 4.

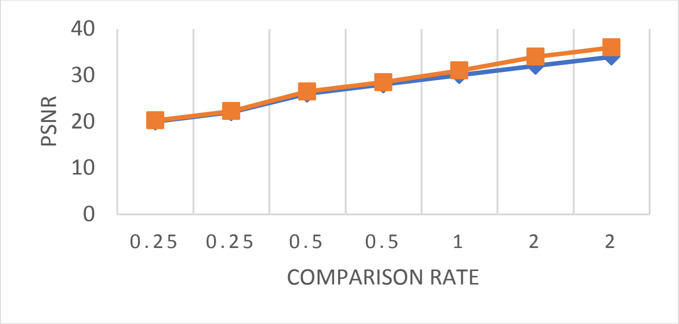

Fig. 4. Comparison of PSNR proposed technique at different compression rates after embedding

6. CONCLUSION AND FUTURE WORK

Success in achieving secrecy using steganographic results from choosing the appropriate method for information hiding. The more the information is sited in the public' s space over the Internet, the more holders of such information are at risk. They need to protect the information from attacks and false depiction. Steganography especially when united with cryptography, provides a most sophisticated means enabling the people to communicate secretly. As the digital technology and Internet have progressed swiftly in recent days, Steganography has developed a lot to achieve better and effective information hiding. The proposed approach combines both the special features of both cryptography and steganography to ensure secure communication for the masses. With the improved approach of amalgaming cryptography with steganography in this article, steganalysis faces new challenges to be solved. Concept of security, secrecy and capacity have to be examined profoundly for qualitative information hiding.

7. REFERENCES

[1]. Rajani Devi.T: Importance of Cryptography in Network Security: International Conference on Communication Systems and Network Technologies, pp. 462 – 467, IEEE Press, New York (2013).
[2]. Johnson.N.F, Jajodia.S: Steganalysis the Investigation of Hidden Information: IEEE Information Technology
[3]. Conference, September (1998).
[4]. Cummins.J, Diskin.P, Lau.S, Parlett.R: Steganography and Digital Watermarking: School of Computer Science, the University of Birmingham (2004).
[5]. Watkins.J: Steganography – Messages Hidden in Bits (2008).
[6]. Luo.W, Huang.F: Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security.201-214 (2010).
[7]. Ge Huayong, Huang Mingsheng, Wang Qian: Steganography and Steganalysis Based on Digital Image, IEEE Trans. International Congress on Image and Signal Processing, pp. 252-255 (2011).

[8]. Nur Hadisukmana, Yosua Kristianto: Steganography Software with Combination of Encryption Algorithms for Multimedia Files, First International Conference on Informatics and Computational Intelligence, IEEE 100 - 105 (2011).

[9]. Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena: Security Improvisation in Image Steganography using DES, IEEE 1094 – 1099(2012).

[10]. Parag Kadam, Mangesh Nawale, Akash andhare, Mukesh Patil: Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique, Proceedings of the International Conference on Pattern Recognition, Informatics and Mobile Engineering February 21-22 IEEE (2013).

[11]. Rijndael Advanced encryption standards,https://www.lri.fr/~fmartignon/documenti/systemesecurite/5-AES.pdf

[12]. Rijndael Advanced encryption standards, https://searchsecurity.techtarget.com/definition/Rijndael

[13]. Rijndael Advanced encryption standards, https://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html

[14]. Rijndael algorithm National Institute of Standards and Technology (NIST), https://ieeexplore.ieee.org/document/1289996

[15]. Classification of steganalysis techniques, https://www.sciencedirect.com/science/article/pii/S1051200410000412

[16]. Sujatha krishnamoorthy Automatic epilepsy detection using hybrid decomposition with multi class support vector method,Multimedia Tools and Applications An International Journal.

[17]. Balaji, B.S., Balakrishnan, S., Venkatachalam, K. et al. Automated query classification-based web service similarity technique using machine learning. J Ambient Intell Human Comput (2020)