ISSN 2395-1621

STEGANOGRAPHY AND CRYPTOGRAPHY METHODS

Rijil Daniel, Pranav Deshmukh, Dhanesh Lunkad, Yogesh Thadani, Anuja Phapale

AISSMS IOIT,SAVITRIBAI PHULE PUNE UNIVERSITY, MAHARASHTRA, INDIA

ABSTRACT

Digital communication has a noticeable and continuous development in many applications in the Internet. The security of data transmitted across a network has turned into a key factor in network performance measures. So, the confidentiality and the integrity of data are needed to prevent from accessing and using transmitted data. The development of data communication needs to be secure and can be achieved by an information security mechanisms. To provide network security there are two mechanisms are Steganography and Cryptography. In this paper, we surveyed a number of papers related to Steganography and Cryptography systems. Capacity of embedding, type of encryption plays crucial role in this techniques. The aim is to provide several studies regarding steganography and cryptography, for the future work.

Keywords— Steganography, Cryptography

ARTICLE INFO

Article History

Received: 8th March 2020

Received in revised form :

8th March 2020

Accepted: 10th March 2020

Published online :

11th March 2020

I. INTRODUCTION

In today's world, secure communication is the basic necessity of every growing area. Each individual wants the confidentiality and integrity of communicating a message. Secure communication is required for privacy. In our day-to-day life, we use different means of communication pathways for transferring and sharing the information which needs to be secured. Security is the main issue in today's world, so there two techniques for information security is Steganography and Cryptography. Steganography is the technique of hiding secret data within a non-secret, file or message in order to avoid detection the secret data is then extracted at its destination. There are many different types of Steganography. Some of them are Image Steganography, Video Steganography, Text Steganography, Video Steganography, Network or Protocol Steganography. Among different types of Image, Steganography is being the preferred medium. In Image Steganography, to achieve confidentiality secret message is hidden in a cover image and cannot be detected by some third party and thus can be used for secure communication.

The key principle of Image Steganography is to preserve the property of the image that means to achieve minimum distortion in the image and achieve confidentiality. While, the Steganography techniques are categorized into six main types which are the spatial domain techniques, such as least significant bit (LSB) based approaches and pixel value differencing (PVD) based approaches, the transform domain techniques such as discrete wavelet transform (DWT), integer wavelet transform(IWT) and discrete cosine transform(DCT), spread spectrum techniques, distortion techniques, masking and filtering techniques, and cover generation techniques. In this paper, we are using the Least Significant Bit (LSB) based approach. During the embedding process, the bytes of pixel matrix of the color image are taken and secret data (any file) is hidden using LSB approximation where LSB's of pixel matrix is replaced by secret data to be hidden, to create stego-image. The stego-image is the image used for communication where secret data is embedded into an image and data is hidden and the stego-image created is not detectable by human vision.

The mean square error (MSE) is used to check and measure the statistical distortion amount between the cover image and stego-image. During the extracting process, the algorithm reads the stego-image and the secret data is extracted from the LSB's of the stego-image and the secret message is reconstructed.

Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can decode the message and understand it. Generally, it is about constructing and analyzing protocols and which are related to various aspects of information security such as data confidentiality, data integrity, authentication, and non-repudiation. Encryption of data is to convert data into an unreadable format. Decryption is the reverse of encryption, it is the transformation of encrypted data back into some intelligible form the data to be encrypted is called plain text. Encryption and Decryption require the use of some secret information, usually referred to as a key that is used to encrypt as well as decrypt. There are two variants they are one is symmetric key and asymmetric key. In symmetric key, the same key is used for encrypting as well as decrypting the data whereas, in asymmetric key, two different keys are used for encryption and decryption. Here, in this paper, we are choosing symmetric key cryptography using Armstrong number where data is encrypted and decrypted using Armstrong number.

II. METHODOLOGIES

Irreversible steganography means once the information to be hidden is embedded on the original image the original image is lost. Reversible steganography is used to recover the original information from stego i.e processed information by extracting secret information. In spatial domain method, the pixel value is directly modified for data hiding. In transform domain, redundancy is reduced and less important areas according to frequency distribution are found. Spread spectrum method is well known approach in digital communication. It consists spreading of the bandwidth of a narrowband signal across a wide band of frequencies. In image steganography, to hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many colour variations, so modifications will not be recognized easily. The most common methods for these alterations include the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These methodologies can be used with varying degrees of success on different types of image files. A very common approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image. To hide a secret message inside an image, a suitable cover image is necessary. Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different way in hiding a message. While masking changes the visible properties of an image, it can be done in such a way that it will not be noticed by human eyes. Masking is faster than LSB insertion with respect to compression, cropping, and some image processing. Masking techniques embed information in selective areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. Cryptography and the Steganography is a classical approach towards data security. In cryptography the data is transformed into an unreadable format during encryption process and during decryption data is again recovered in its original format. On the other hand, in data steganography the data is encapsulated in a specific format to hide the information and during the recovery of data the information is recovered in its original format without any modification on cover.

III. LITERATURE SURVEY

In [1], they have mentioned how undetectability and capacity are the two important factors to be considered in image steganography. Here they have shown that in traditional Least significant bit method the secret data bits are uniformly embedded in the cover image even if the cover image is not uniform (in terms of pixels) and how this could affect the detection.

Proposed Method: Here they propose a method which in which the capacity of each pixel is not uniform instead it is decided by detailed analysis of the cover image by an algorithm and then the embedding is done accordingly hence making its steganalysis difficult. More on the algorithm first they initialize some parameter which they use for data processing and region selection. Region is selected based on the smooth and sharp areas of the image and also then the embedding capacity is calculated. If the capacity is large enough for secret data then the hiding is performed and if the capacity isn't large enough the scheme is revised and the parameters are changed and this process is carried until data can be embedded completely. For extraction it first extracts the parameters and then it preprocesses the data using shared keys and then regions are extracted and hence we get the secret data.

Drawbacks: The main drawback of this method is embedding capacity (1bpp [average]) which is far less than the embedding capacities of the recent methods. Steganalysis of the method using the entropy distribution of the image is possible and hence we can extract the secret data by those entropy patterns.

In [2], the whole algorithm lies behind the entropy distribution of the image that is intensities of each and every pixel. When the secret data is embedded intensities change and hence steeganalysis can be done easily.

Proposed Method: In this method basically first we calculate entropies of the image that is intensities of each pixel of the image then in the next step we form a graph of the intensities and then if we can get our hands on the cover image or the entropy graph of the cover image we can detect the drop or rise in intensities and hence we can find out the detection of secret data. And also by finding the difference between the entropies we can also extract the secret data.

Drawbacks: This method doesn't work on all types of steganographic methods that exist. This method has poor accuracy as compared to other methods.

In [3], the author has firstly taken into consideration the robustness of the existing algorithm to avoid steganalysis and hence they put forward a method which would be able to make the method much more reliant and robust. They name the method as Coverless image steganography.

Proposed Method:
In their method firstly the features are extracted from the image then by converting the secret data into binary they are cut into small blocks of size M and further by using that an inverted image index is established. Then the secret information is embedded through these mapping rules and hence the cover image is not modified in the steganography process. This method can effectively resist various steganalysis algorithms. At the receiver side during extraction the entire sequence is extracted using the mapping rules and those are joined together to form the complete information.

Drawbacks: Low embedding capacity as compared to the latest methods. Various types of data can't be embedded

In [4], Permutation Steganography allows ordering of set of n elements, in order, to avoid distortion of the stego media. It also uses the 2 basic steps: Encoding and decoding (embedding and extraction) of the secret message. This technique requires n numbers of sequence elements to perform data hiding. we could decide which sequence element to be considered for embedding data.

Encoding Section: ----------
For example, if there are 3 sequence elements: b, a, c Consider secret data: 110 Initially, they sorted (a, b, c) and then using the above formula (considering n = 3 for this case) m would equals to 1 (3-2^1). Then according to the indexing of the sorted sequence we could add 'b' to the stego sequence buffer as b has the index 1 in the sorted sequence.
Further, we read 1-bit word from the secret data and check its decimal value. In this case, the value would result in 1 and if value < m, then we could pick the next bit of the secret data until value is less than m, else we could directly jump to the next step. Then as value is becomes equal to m, we remove the sequence element and store in the stego sequence element and then b is removed from the sorted sequence and stored in the stego sequence and b is replaced with c in the sorted sequence.

So, the sorted sequence is a, c and stego sequence is b and the secret data is 10. Now again we will calculate the value of m and follow the above procedure until the embedding is performed.
Result: Stego Sequence: b, a, c (Encoded secret data).
Decoding Section ----------
Considering the stego sequence obtained in the above result we will retain the original secret message. First we calculate the parameters k and mm where k = log 3 = 1 and m = 3-2^1 = 1. Second we pick the first stego element (i.e. b) which has the value 1 in the sorted sequence and next we consider 1 bit-word extraction of encoded message "1". As value (1) is equal to m we cannot read an extra bit hence jump to next step. In the next step we consider the next stego sequence element (a) for extraction. We again read 1 bit-word of the message and now we get "11" and finally after doing it for c we get "110" and we have decoded the original message.
Time Complexity: O(n)

Drawbacks:
The author has tried to improvise the embedding capacity but will require large number of sequence elements for encoding large amount of data which will result in more time.

In [5], Steganalysis of MBNS (Multiple base notational system) steganography is basically detection of steganography performed on images pixels using MBNS method. In the MBNS steganography technique, the secret data is converted into symbols (in a notational system) with multiple systems. The pixels of the cover image are modified in such a way that dividing the pixel values by their bases would result in a remainder that equals to the symbols. The detection technique used in this paper not only detects the MBNS steganography but also estimates its embedding rate. The technique basically works as follows:
* It considers a pixel value p (i, j) as input.
* Using some mathematical equations, it computes all the bases and the corresponding remainders for all input image pixels.
* Then sorts the bases according to their frequencies in descending order.
* And after some processing outputs the value 0 or 1, where 0 indicates no data embedding done and 1 indicates that some data is embedded in the pixel considered. * This is repeated for all the pixels.

Drawback:
This technique is particularly based on detection of MNBS steganography and cannot give expected results for other steganography techniques.

IV. FUTURE DIRECTIONS

A system can be developed to hide the information into an image by combining two methods: Steganography and Cryptography and thereby achieving its advantages. In this method, first, it encrypts the information to be hidden using the Armstrong number using a symmetric key method and hide the encrypted information into an image using LSB approach at the sender side and then, at the receiver side, the encrypted information is extracted and then it is decrypted. Any type of file can be hidden into a cover image. Thus, two levels of security is achieved which makes our system stronger.

Existing methods of steganography will be advanced as per necessity. But now is the age of digital data. So, in the near future, the most important use of steganography techniques will be in the area of digital data. Content providers very protective of their copyrighted works against illegal actions and digital watermarks provide a way of tracking the owners of such work material. It will enable the content provider to start legal actions against the malpractice, as it can be tracked down now.
Steganography can be useful for wrong motives as well. Government may increase restrictions on this technology to reduce the misuse in future. Especially in time with possibility of terrorist attacks and other threats.

V. CONCLUSION

Steganography is very important and old technique regarding information security. Steganography can work with various kinds of data or information (Text, image, audio, video). All the famous traditional methods such as LSB method are being advanced and modified as new and advanced steganalysis techniques are being introduced. Nowadays, researchers are working on machine learning techniques as well. Large and useful training sets can be major advantage for such techniques. The main goal in steganography is to increase capacity for hiding information and improve quality of stego material. Among various steganography techniques, one should select appropriate technique to get better result.

REFRENCES

[1] Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE (2010) “Edge Adaptive Image Steganography Based on LSB”

[2] “Steganalysis based on the entropy distribution of the image and identifying the method used for encoding” IEEE paper (2010)

[3] Xiang Zhang, Fei Peng, IEEE Member, and Min Long (2018) “Robust Coverless Image Steganography based on DCT and LDA”

[4] Nien-ching Huang, Meng-tsan Li, Chungming Wang (2009), “Toward optimal embedding capacity for permutation steganography”

[5] Bin Li, Student Member, IEEE, Yanmei Fang, and Jiwu Huang, Senior Member, IEEE (2008) “Steganalysis of Multiple-Base Notational System Steganography”

[6] K. Upendra Raju and N. Amutha Prabha, “ review of reversible steganography” FEBRUARY 2018 ISSN 1819-6608 ARPN Journal of Engineering and Applied Sciences.

[7] Pratiksha Sethi, V.Kapoor, “A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography”, International Journal of Computer Applications, June 2016

[8] E.Emad, A.Safey, ARefaat, Z.Osama, E.Sayed, E.Mohamed. “A secure image steganography algorithm based on least significant bit and integer
wavelet transform”, Journal of Systems Engineering and Electronics,2018

[9] s.chakraborty,anand jalal,charul bhatnagar, “Secret image using grayscale payload decomposition and irreversible image steganography”, Journal of information security and applications,2013

