SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 5, NO. 6
ISSN: 2054 -7420

Cryptography and Steganography: New Approach

[1]Ahmed AL-Shaaby, [2]Talal AlKharobi
College of Computer Sciences and Engineering,
King Fahd University of Petroleum and Minerals,
Dhahran, Saudi Arabia
g201408620@kfupm.edu.sa, talalkh@kfupm.edu.sa

ABSTRACT

Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security. In this paper, we survey a number of methods combining cryptography and steganography techniques in one system. Moreover, we present some differences between cryptography and steganography. The aim of this paper is to develop a new approach to hiding a secret information in an image or audio or video, by taking advantage of benefits of combining cryptography and steganography. In this method first, the message is encrypted by using AES algorithm and hashed the key using SHA-2 to prevent from attacks. After that, we performed some modifications on LSB algorithm by adding a key to make hiding process non sequential. Results achieved indicate that our proposed method is encouraging in terms of robustness and security.

Keywords: Steganography, Cryptography, Least Significant Bit (LSB), encryption, decryption, Stego image, Color image, Random embedding.

1 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 [1]. The significance of network security is increased day by day as the size of data being transferred across the Internet [2]. Cryptography and steganography provide most significant techniques for information security [3].

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 [2]. Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks [4]. A solution for this issue is using the advantage of cryptography and steganography combined in one system [5, 3].

This paper presents a historical background of the art of cryptography and steganography and shows the differences between these techniques in Section 2, A literature review about methods which combined

DOI: 10.14738/tnc.56.3914
Publication Date: 5th December 2017
URL: http://dx.doi.org/10.14738/tnc.56.3914

steganography techniques and cryptography techniques is outlined in section 3. In Section 4, we describe the proposed methods. Section 5 shows the results and the implementation of this method. Section 6 shows the conclusion.

2 Background

Cryptography and steganography are two approaches used to secure information, either by encoding the information with a key or by hiding it [6, 7, 8, 1]. Combining these two approaches in one system gives more security [5, 9]. It is useful to explain these approaches and discuss the benefits combining them.

2.1 Cryptography

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like: confidentiality, privacy, non-repudiation, key exchange, and authentication. Figure 1 shows the cryptography system [10].

There are two types of cryptographic schemes for securing the data. These schemes are often used to reach the objective: public-key cryptography, secret key cryptography, and hash functions. The length and type of the keys used depend on the type of encryption algorithm [10].

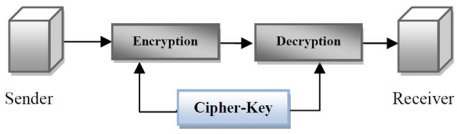

Figure 1: Cryptography System [11]

2.1.1 Symmetric / Secret Key Cryptography

The technique of Secret key encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all sides encryption and decryption secret data. The original information or plaintext is encrypted with a key by the sender side also the similarly key is used by the receiver to decrypt a message to obtain the plaintext. the key will be known only by a people who are authorized to the encryption/decryption. [12].

However, the technique affords the good security for transmission but there is a difficulty with the distribution of the key. if one stole or explore the key he can get whole data without any difficulty. An example of Symmetric-Key is DES Algorithm [12].

2.1.2 Asymmetric / Public Key Cryptography

We can call this technique as asymmetric cryptosystem or public key cryptosystem, this technique use two keys which are mathematically associated, use separately for encrypting and decrypting the information.

In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. all keys are needed for the technique to run. The key used for encryption is stored public therefore it's called public key, and the decryption key is stored secret and called private key. an example of Asymmetric-Key Algorithms is RSA RSA [10].

2.2 Steganography

Can be defined as the science of hiding and communicating data through apparently reliable carriers in attempt to hide the existence of the data. So, there is no knowledge of the existence of the message in the first place. If a person views the cover which the information is hidden inside of he or she will have no clue that there is any covering data, in this way the individual won't endeavour to decode the data. Figure 2 shows the steganography system overview [10].

The secret information can be inserted into the cover media by the stego system encoder with using certain algorithm. A secret message can be plaintext, an image, ciphertext , or anything which can be represented in form of a bitstream. after the secret date is embedded in the cover object, the cover object will be called as a stego object also the stego object sends to the receiver by selecting the suitable channel, where decoder system is used with the same stego method for obtaining original information as the sender would like to transfer [10]. There are various types of steganography.

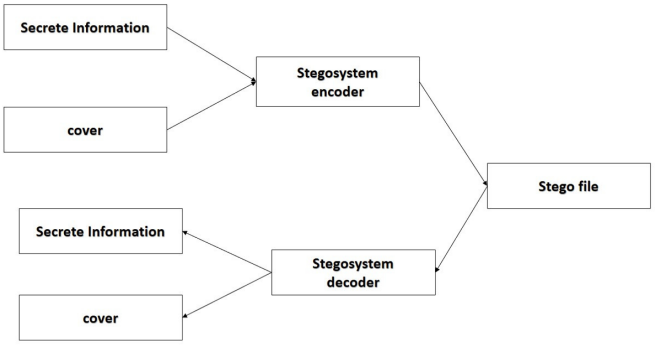

Figure 2: Steganography System

2.2.1 Text Files

The technique of embedding secret data inside a text is identified as text stego. Text steganography needs a low memory because this type of file can only store text files. It affords fast transfer or communication of files from a sender to receiver [1].

2.2.2 Image Files

It is the procedure in which we embed the information inside the pixels of image. So, that the attackers cannot observe any change in the cover image. LSB approach is a common image steganography algorithm [1].

2.2.3 Audio Files

It is the process in which we hide the information inside an audio. There are many approaches to hide secret information in an audio files for examples Phase Coding, LSB [1].

2.2.4 Video Files

It is the process of hiding some secret data inside the frames of a video [1].

2.3 Cryptography vs Steganography

Table 1 shows the differences between the steganography and cryptography using some criteria. The comparison is based on, Definition, Objective, Carrier, Input file, Key, Visibility, Security services offered, Type of Attack, Attacks, Result, Applications.

Table 1: Cryptography vs Steganography

Criteria/Method	Steganography	Cryptography
Definition	Cover writing [7, 1]	Secret writing [7, 1]
Objective	Maintaining existence of a message secret ,Secret communication [7, 1, 5]	Maintaining contents of a message secret ,Data protection [7, 1, 5]
Carrier	Any digital media [7, 1, 6, 10, 8]	Usually text based [7, 1, 6, 10, 8]
Input file	At least two [6]	One [6]
Key	Optional [6, 7, 8, 1]	Necessary [6, 7, 8, 1]
Visibility	Never [6, 1, 7]	Always [6, 1, 7]
Security services offered	Authentication, Confidentiality, Identification [10]	Confidentiality, Identification, Data Integrity and authentication Non-repudiation [6, 7, 1, 10]
Type of Attack	Steganalysis: Analysis of a file with an aim of finding whether it is stego file or not [6, 1, 10, 8]	Cryptanalysis [6, 1, 10, 8]
Attacks	Broken when attacker reveals that steganography has been used. known as Steganaly-sis. [6, 5, 7, 1]	Broken when attacker can understand the secret message. known as Cryptanalysis [6, 5, 7, 1].
Result	Stego file [6, 1, 8]	Ciphertext [6, 1, 8]
Applications	Used for securing information against potential eavesdroppers [10]	Used for securing information against potential eavesdroppers [10]

2.4 Benefits Of combine the Steganography and Cryptography

It is noted that steganography and cryptography alone is insufficient for the security of information, therefore If we combine these systems, we can generate more reliable and strong approach [9].

The combination these two strategies will improve the security of the information secret. This combined will fulfill the prerequisites, for example, memory space, security, and strength for important information transmission across an open channel. Also, it will be a powerful mechanism which enables people to communicate without interferes of eavesdroppers even knowing there is a style of communication in the first place. [5].

3 Literature Review

As we said the significance of network security is increased day by day as the size of data being transferred across the Internet. This issue pushes the researchers to do many studies to increase the ability to solve security issues. A solution for this issue is using the advantage of cryptography and steganography combined in one system. many studies propose methods to combine cryptography with steganography systems in one system. these methods were deceased in previous surveys available on the topic. This survey [1] was published in 2014, it aims to give an overview of the method proposed to combine cryptography with steganography systems. In this survey, the authors introduced 12 methods which are combined steganography and cryptography and made a comparative analysis. This comparative has been implemented on the basis of the requirements of security i.e. authentication, confidentiality, and robustness. Another survey [12] was published in 2014, this survey presented many steganographic techniques combined with cryptography, AES Algorithm, Alteration Component, Random Key Generation, Distortion Process, Key Based Security Algorithm.

There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for the security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together.

In [13], proposed an encrypting technique by combining cryptography and steganography techniques to hide the data. In cryptography process, they proposed an effective technique for data encryption using one's complement method, which we called as SCMACS. It used a symmetric key method where both sender and receiver share the same key for encryption and decryption. In steganography part, we used the LSB method that is used and mostly preferred.

In [14], authors proposed a highly-secured steganography technique by combining DNA sequence with Hyperelliptic Curve Cryptography. This approach executes the benefits of both techniques to afford a high level of security communication. Also, it uses the benefits of both DNA cryptography and Steganography. This algorithm tries to hide a secret image in another cover image by convert them into DNA sequence using the nucleotide to the binary transformation table. On the sender side, the embedding method includes three steps. First, they convert the values of a pixel of both the cover image and secret image to their respective DNA triplet value utilizing characters to the DNA triplet conversion. Secondly, they convert the triplet values to binary values format. In the final stage, apply the XOR logic between binary values of both secret image and cover image to generate a new image which called stego image.

In [15], authors presented a new technique called multi-level secret data hiding which integrates two different methods of encryption namely visual cryptography and steganography. The first step of this method thy used a method called halftoning which is used to reduce the pixels and simplify the processing. After that visual cryptography is performed that produces the shares which form the first level of security and then steganography in which thy used the LSB method to hide the shares in different media like image, audio, and video.

The paper at [16] presented a method based on combining both the strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. An encryption technique is employed for encrypting a secret message before encoding it into a QR code. They used AES-128 key encryption technique. they encrypted a message, in

UTF-8 format is converted into base64 format to make it compatible for further processing. The encoded image is scrambled to achieve another security level. The scrambled QR code is finally embedded in a suitable cover image, which is then transferred securely to deliver the secret information. They utilized a least significant bit method to accomplish the digital image steganography. At the receiver's side, the secret data is retrieved through the decoding process. Thus, a four-level security has been rendered for them a secret message to be transferred.

In [17] authors presented an image steganography method. At first, they used the DES algorithm to encrypt the text message. They used a 16 round and with block size 64-bit. After that the K-Means Clustering of The Pixels method which clusters the image into numerous segments and embedded data in every segment. There are many clustering algorithms use for image segmentation. Segmentation includes a huge set of information in the form of pixels, where every pixel additional has three components namely red, green and blue(RGB). After the formation of clusters, the encrypted text is separated into K number of segments. These segments are to be hidden in each cluster. They used the LSB (Least Significant Bit) method for this purpose.

In [18], authors said that Cryptography and Steganography alone cannot be used for transmission of data because each has their own weaknesses. So, they proposed a system, both the technologies are used together to create a nearly impossible way for third parties to breach the system and gain confidential data. The system used a latest TwoFish algorithm for encryption while a new approach for performing the steganography is used which called Adaptive B45 steganography technique.

In [19], authors presented a method to extend the embedding capacity and to enhance the quality of stego image. The Adaptive Pixel Value Differencing which is an improved form of Pixel Value Differencing was utilized as the Steganographic system although AES was utilized as the Cryptographic system. In this method, they used an image as a cover to hide the secret data inside. This cover should be a grayscale image. therefore, pixel size must be 256*256. If the size of a pixel was high they brought it to this range. They checked if the cover image is a color image they changed it into the grayscale range. They used APVD algorithm to embed the data into the cover image. The result gotten after hiding the data called stego image. They used AES algorithm to encrypt stego image.

In [20], 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.

In [21], authors performed a modern method in which use Huffman encoding to hide data. They took a gray 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.

In [22], authors suggested a new steganographic technique based on gray-level modification for true color images using a secret key, cryptography and image transposition. Both the secret key and secret information are firstly encrypted using multiple encryption algorithms (bitxor operation, stego key-based encryption, and bits shuffling); these are, later, hidden in the cover image pixels. In addition, the input

image is changed before data hiding. Image transposition, bitxoring, stego key-based encryption, bits shuffling, and gray-level modification introduces five various security levels to the suggested technique, making the recovery of data is very difficult for attackers.

In [23], propose approach which used blowfish Encryption to encrypt the secret information before embedding it in the image using LSB method.

In [24], 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.

In [25], the research discussed hiding information using steganography and cryptography. A new approach is explained to secure data without decrease the quality of an image as a cover medium. The steganographic method is used by finding the similarity bit of the message with a bit of the Most Significant Bit(MSB) image cover. They used divide and conquer method for finding the similarity. The outcomes are bit index position, later they encrypted using cryptographic. In this article, they used DES (Data Encryption Standard) algorithm.

In [26], authors proposed a new method. First, the secret message is changed into cipher text using RSA algorithm and next they hide the cipher text in audio using LSB audio steganography technique similarly. At receiver, first, cipher text is extracted from audio then decrypted it into a message by using RSA decryption. So, this technique combines the characteristic of both cryptography and steganography and provides a higher level of security.

In paper [27], authors used BLOWFISH cryptography Algorithm to encrypt a secret image. Because BLOWFISH is faster and stronger, provides good performance when compared with RC6, RC4, DES, 3DES, AES. They selected a secret image in BMP format and encrypted by BLOWFISH algorithm. Then, they used LSB technique to embed encrypted image into video frames using. This method affords authenticity, integrity, confidentiality and non-repudiation.

The paper [28], is similar to the method mentioned in [27] but the only difference is that here the text is selected to be a secret message instead of image and encrypted using BLOWFISH Algorithm. Next, they used the image to be a cover object and use the LSB technique to embed the encrypted text into this cover.

In [29], authors proposed new strategy employs RSA algorithm with 128-byte key size for encrypting the secret information before embedded it into a cover image and use F5 steganographic algorithm to embed the encrypted message in the cover image gradually. they selected chosen Discrete Courier Transform (DCT) coefficients randomly to embed the secret message into it by using F5 algorithm. They applied matrix embedding to reduce the changes to be made to the length of a specific message, this strategy gives faster speed, high Steganographic capacity, and can prevent observed and analytical attacks.

In [30], authors have proposed a novel visual cryptographic technique. This technique is suitable for both Grayscale and Bitmap Color images. In this approach, the theory of Residual Number System was utilized based on Chinese Remainder Theorem for share creation and shares stacking of a given image. First, they embedded a secret image in a cover image to make stego-image. A pixel 8 bit of a Stego-image is selected and added with an 8-bit key to produce a cipher pixel. They utilized additive mod 255 algorithm. They used a pseudo-random number generator and Mixed Key Generation technique to generate the key.

Secondly, after they encrypted the stego image they mapped cipher pixel into a Residue Number System of n pieces. Finally, they collected and send n pieces the target. This approach is extremely fast, secure, reliable, efficient and easy to implement.

In [31], the combination of cryptography and Image Steganography has been reached by utilizing both AES and LSB algorithm. they utilized the LSB technique to embed the confidential information into an image file and they used AES algorithm for encrypting the stego image. Finally, authors conclude that this technique is effective for secret communication and provides the better security.

The authors in [32], made a comparative study of steganography and cryptography. They surveyed a number of methods combining cryptography and steganography techniques in one system. Moreover, they presented a classification of these methods and compare them in terms of the algorithm used for encryption, the steganography technique and the file type used for covering the information. consequently, they conclude that the methods which start with cryptography first are more common than methods which start with steganography, and provide better security with less exposing of the encrypted data. The only advantage of methods which start with steganography is providing more capacity for the secret information.

4 Proposed Method

In this section, we will discuss proposed method which combines two information hiding techniques. which are Cryptography and Steganography. In this proposed method first, the message is encrypted by use AES algorithm and hashed the key using SHA-2 to prevent from attacks. After that, we use the modified LSB technique to embed the encrypted information in image, video or audio. The receiver must implement the key which is hashed in sender side. So, this technique combines the features of both cryptography and steganography and provides a higher level of security. It is better than either of the technique used separately. The secret data can be hidden in any type of media which affords more security. There will be an agreement between the sender and the receiver about the key for the concealment algorithm as well as the key for the encryption algorithm or these keys may be exchanged by a secure communication method. Our method starts by encryption first then hide encrypted data. Figure 3 shows the presentation of sender side of this method and Figure 4 shows the presentation of receiver side of this method.

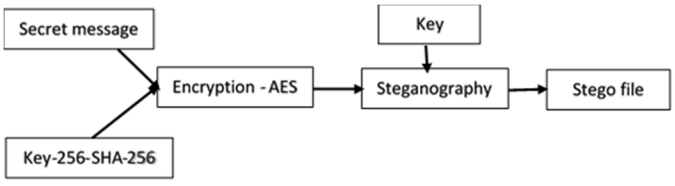

Figure 3: Sender Side

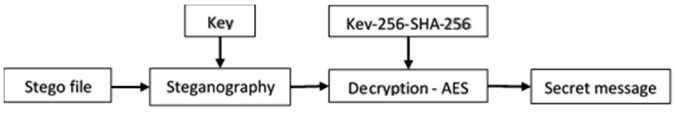

Figure 4: Receiver Side

4.1 Sender side

The Sender side consists of cryptographic and cryptographic stages. This method starts with cryptographic then steganography.

4.1.1 Encryption Stage

In encryption stage, we use AES (Advanced Encryption Standard) algorithm with key 256 bit and Block Size 128 bit to encrypt secret message. This technique takes a 14-character password (8 bits per character) for encrypting the message, which is communicated to the receiving end for decryption. The encrypted message, in UTF-8 format, is converted into a base64 format to make it compatible for further processing, which is then written into the file and stored for further processing. and hashed the key using SHA-2(SHA-256) to prevent from attacks. This encrypted data will be used in steganography stage.

Input= private key+ secret message (1)

Output= encrypted message (2)

4.1.2 Steganographic Stage

In stenography stage, we use LSB (List Significant Bit) algorithm with some modification to hide information (encrypted data from cryptography stage) inside files. In our experiment, we use the image as cover to present our method, but this method can be applied to other files such as audio, and video. The general LSB method used to hide secret information into a file; the last bit in each pixel or sample or frame used sequentially to hide one of the binary stream bits Encryption of the cover image. But in our method, we purpose some modification to enhance LSB. So, we make the hiding operation randomly instead of sequentially by applying some of the mathematics operations depend on key given by the user Proposed method:

Input= encrypted message + private key+ cover image (3)

Output= stego-image (4)

1. Read the secret message and the key.
2. Convert all secret message to binary format.
3. Add a special code at the end of the text, to take advantage of when retrieving the concealment.
4. Choose the appropriate image size for the hiding process.
5. Read the character from the text and find the ASCII formula corresponding to it in bytes, then divide the byte into three parts segment the first contains (2) the first two parts and the second and third parts each contains (3) bits in the sequence.
6. Read the first pixel of image.
7. Convert the pixel value to binary format.

For example, first pixel has value in R colour = 200, G colour =210, B colour=186. And the key =9. Also, the secret message is (K) So the colour value in binary for each colour as follow: Red= (1100 1000)

Green= (1101 0010)

Blue= (1011 1010)

And the secret message = (0110 1011)

8. Take two bits of the secret message and hide it in LSB of colour R and take another three bits and hide it in LSB of colour G and three bits and hide it in LSB of colour

   B. The values of new colour will be as follow:

   R= (1100 1011) =203

   G= (11010010) =210

   B= (1011 1011) =187

9. Calculate the space of hiding by taking four bits from any colour and add it with the key.

   For example, if we take from G (0010) = 2,

$$S= (N)2 +(Key). \quad (5)$$

   The space S=2+9=11.

10. Calculate the next pixel to hide information inside it. As we now we can access to pixels by using axis (X, Y).

$$\text{So next pixel} = (X, Y+S). \quad (6)$$

    For example, if we are in pixel (5,34) the next pixel will be (5,34+11) = (5,45).

    So, the next potion to hide in it is pixel (5,45).

11. Repeat steps (5,6,7,8,9,10) until the code for the end of the text appears.

4.2 Receiver side

Receiver side consists of steganography and cryptography stages. In receiver side we will first extract embedded data then decrypt it.

4.2.1 Stenography Stage

In the receiver side, we start with steganography then cryptography. We will use the same steps which are used in sender side.

$$\text{Input= stego-image+ private key} \quad (7)$$

$$\text{Output= encrypted message} \quad (8)$$

4.2.2 Cryptography Stage

In cryptography stage, we use the data which is extracted from stego file and use AES (Advanced Encryption Standard) algorithm with key 256 bit and Block Size 128 bit to decrypt it. We will use the same steps which are used in sender side.

$$\text{Input= encrypted message + private key} \quad (9)$$

$$\text{Output= secret message} \quad (10)$$

5 Experimental Results

Experimental results of the proposed method are presented in this section; they are achieved by a program written in C# language. The tests with colour image as cover ran on a personal computer. Figure 5 present the interface of our application and how the application work if the keys is correct. But if the keys are not correct the result will be as shown in Figure 6.

Figure 5: Correct Key

Figure 6: Incorrect Key

The method proposed has proved successful in concealing various types of text in colour images. The hash distance between image pixels reduces the probability of detecting hidden text because the distribution depends on a secret key, in addition to an unstable displacement distance. The methods that use sequential hiding at a constant pace are more likely to be discovered and suspicious of snipers or hackers. Using the value of the key with the value of a portion of the resulting image element after the masking process enables the control of the hash distance and thus balances the size of the text to be hidden and the size of the cover image. The percentage of concealment in this method is less compared to the traditional methods of the existence of space left without hiding because of adopting the mechanism of skimming in the process. It is preferable to use images with many details (ie high-text images) in the process of concealment. Performing any process of compressing or improving the image containing the hidden text or changing its extension will result in Lost all or part of the hidden text and cannot be retrieved in full. To increase the efficiency of concealment in the colour image, it is possible to distribute the concealment of the three parts on the three colours on that the amount of skewing for each colour is calculated separately, so that each part of the character to be hidden in an item different pixel of the image as this reduces the possibility of detection. In this proposed method, video files are the better cover object than image and audio. Because of their high capacity.

6 Conclusion

In this paper, the concepts of security of digital data communication across the network are studied. This paper is designed for combining the steganography and cryptography features factors for better performance. We performed a new steganography method and combined it with AES algorithm. We performed our method on image by implementing a program written in C# language. The tests with colour images as cover ran on a personal computer. The method proposed has proved successful in hiding various types of text in colour images. The hash distance between image's pixels reduces the probability of detecting hidden text because the distribution depends on a secret key, in addition to an unstable displacement distance. We concluded that in our method the video files are the better cover object than image and audio. Because of their high capacity. Results achieved indicate that our proposed method is encouraging in terms of security, and robustness.

REFERENCES

[1] M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.

[2] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.

[3] 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.

[4] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975–8887) Volume, 2010.

[5] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp. 978–960, 2014.

[6] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013.

[7] N. Khan and K. S. Gorde, "Data security by video steganography and cryptography techniques," 2015.

[8] M. K. I. Rahmani and M. A. K. G. M. Mudgal, "Study of cryptography and steganography system," 2015.

[9] C. P. Shukla, R. S. Chadha, and A. Kumar, "Enhance security in steganography with cryptography," 2014.

[10] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.

[11] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607–611.

[12] H. Sharma, K. K. Sharma, and S. Chauhan, “Steganography techniques using cryptography-a review paper,” 2014.

[13] A. Dhamija and V. Dhaka, “A novel cryptographic and steganographic approach for secure cloud data migration,” in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 346–351.

[14] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, “An improved level of security for dna steganography using hyperelliptic curve cryptography,” Wireless Personal Communications, pp. 1–22, 2016.

[15] S. S. Patil and S. Goud, “Enhanced multi level secret data hiding,” 2016.

[16] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, “Enhanced security in steganography using encryption and quick response code,” in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016, pp. 2308–2312.

[17] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, “Image steganography method using k-means clustering and encryption techniques,” in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016, pp. 1206–1211.

[18] A. Hingmire, S. Ojha, C. Jain, and K. Thombare, “Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption,” International Educational Scientific Research Journal, vol. 2, no. 4, 2016.

[19] F. Joseph and A. P. S. Sivakumar, “Advanced security enhancement of data before distribution,” 2015.

[20] B. Padmavathi and S. R. Kumari, “A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution,” IJSR, India, 2013.

[21] 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.

[22] K. Muhammad, J. Ahmad, M. Sajjad, and M. Zubair, “Secure image steganography using cryptography and image transposition,” arXiv preprint arXiv:1510.04413, 2015.

[23] T. S. Barhoom and S. M. A. Mousa, “A steganography lsb technique for hiding image within image using blowfish encryption algorithm,” 2015.

[24] 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.

[25] M. A. Muslim, B. Prasetiyo et al., “Data hiding security using bit matching-based steganography and cryptography without change the stego image quality,” Journal of Theoretical and Applied Information Technology, vol. 82, no. 1, p. 106, 2015.

[26] A. Gambhir and A. R. Mishra, “A new data hiding technique with multilayer security system.” 2015.

[27] M. H. Sharma, M. MithleshArya, and M. D. Goyal, "Secure image hiding algorithm using cryptography and steganography," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, pp. 2278–0661, 2013.

[28] A. Singh and S. Malik, "Securing data by using cryptography with steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013.

[29] M. Mishra, G. Tiwari, and A. K. Yadav, "Secret communication using public key steganography," in Recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014, pp. 1–5.

[30] R. H. Kumar, P. H. Kumar, K. Sudeepa, and G. Aithal, "Enhanced security system using symmetric encryption and visual cryptography," International Journal of Advances in Engineering & Technology, vol. 6, no. 3, p. 1211, 2013.

[31] D. R. Sridevi, P. Vijaya, and K. S. Rao, "Image steganography combined with cryptography," Council for Innovative Research Peer Review Research Publishing System Journal: IJCT, vol. 9, no. 1, 2013.

[32] S. Almuhammadi and A. Al-Shaaby, "A survey on recent approaches combining cryptography and steganography," Computer Science Information Technology (CS IT), 2017.