International Journal on Emerging Technologies **10**(2): 156-158(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Novel Steganography Methodology Applied in Transposition Cipher for Hiding Text message

P. Rajendiran[1], K.R. Sekar[1], C. Ramesh[2] and R. Manikandan[1]
[1]School of Computing, SASTRA Deemed University, Thanjavur, India
[2]Department of Computer Science & Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India

(Corresponding author: K.R. Sekar)

(Received 08 May 2019, Revised 10 July 2019 Accepted 18 July 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Secret data has been hidden in the image using the least significant bit of digital Steganography. In the present scenario, security is much appreciated in the growing eventual world. An enhanced least significant technique used in the Transposition Cipher technique to format the plaintext into matrix format and permitted to get the ciphertext. The transposition matrix text is obtained by the XOR operation with the key produced through hyper elliptic curve cryptography. Reverse permutation gets back in the other end as a plain text. The ciphertext is spread out on the image by replacing the least significant bit of pixel information based on the Knight Tour Algorithm. The algorithm is based on the traversal of the Knight on an 8 x 8 chessboard. Since using the Transposition Cipher will increase the efficiency of the encryption algorithm to safeguard the hidden message instead of the existing symmetric algorithm which is prone to intruder attack. The research work includes the increased security level of simple least significant bit technique. By using compression technique it is not only increased payload capacity but also the increased robustness and quality. Encryption technique randomizes the message by providing additional security to the secret message.

Keywords: Staganography, Knight Tour, CipherText,Least Significant Bit and Crytopgraphy

I. INTRODUCTION

Usually steganography is the method used to hide the data inside the images for higher security issues. It is most popular way to do such a type of thing in the recent past. But doing such a type of a operation not lead to extra complexity to the model. Minimizing the complexity of the model another factor should be implemented that leads to optimize our research work. The image cannot be disturbed much, at the same time the message is embedded inside the image in the Least Significant Bit (LSB). In the unsecured network sending the message is not the encouraging way because of the intruders, hackers and Spoofing personalities. Now the latest technologies like TCPDUMP, METASPLOIT and NETCAT tools are available to know the vulnerability of our packets and every packet is safeguarded by the packet analyzer. Tcpdump is not only to safeguard our system but it can do some sabotage to the target machine. Higher level of security will be provided to the packets which are travelling through the unsecured network using the steganography.

Steganography is the communication protocol where messages are to be shared among users through the network [1]. The steganography hides the existence of a hidden message where Cryptography randomizes the hidden message. It is the type of art that hides the existence of the message in the cover. The cover to be used of any format example text, audio, image, video, etc. It is derived from the Greek word 'Stefanos' meaning covered or secret writing. The secret data is inserted into the cover image and the embedded image is called Stagno image. The earlier methods manipulated the message that is to be transmitted so that the message could not be understood by the third party even if the message was unintentionally retrieved by them through any means. But it is not enough because the original message was retrieved by brute force techniques. In order to overcome, the concept of key generation was introduced. The sender encrypts the message using the key and the decryption was done by the receiver on the message with the help of the key used in encryption. The flaw found in the technique was the transfer of the key from the sender to the receiver, which is vulnerable to attacks. So new techniques were formulated in which the same key was generated at both the ends without the need of transmitting the actual key. These techniques were designed based on the special property processed by the mathematical elliptic curve. The information to be transmitted is embedded in multimedia objects like images, audios, and videos. The embedded message will not disrupt the original quality of the multimedia object because the mechanism would be done in such a manner that the human eye and ear cannot distinguish the minor changes that have been caused through the technique [5]. The robustness was achieved by the embedding secret information in the least significant bit position of the multimedia object [6]. The combination of the embedded modern technique of encryption would meet the requirement and provides almost security to the transferred message.

II. LITERATURE SURVEY

The existing method in the embedded phase processed the three procedures. In the first stage, Vigenere encryption is used for creating the cipher text [8]. The Vigenere can be split by using the Friedman test, Frequency Analysis, and Key Elimination test. In the next stage, Lempel Ziv Welch compression used to compress the text to increase the occupational capacity. However, LZW compression is less efficient as the dictionary size because of too large and requires searching mechanisms to determine the code for the character for Encoding and Decoding. The Embedding phase involves the replacement of the data bit in the least significant bit (LSB) bit. The Least Significant Bit in the embedded text cannot be identified by the human eye and cannot visualize the smaller distortion that occurs when LSB bits are changed. The SB pixel is opted for embedding the image. However, simple or conventional LSB is less secure as it is easy to obtain secret data. Once the intruder finds that a secret message is embedded in the image, anyone can easily get the message bits from the image. It leads to create security issues. There is increased payload capacity and imperceptibility in LSB is not secured. It would be easier to extract the message from the cover image and secret data would be revealed to the intruders [9]. In order to overcome the drawbacks, the novel LSB technique has been designed for considering the security issues.

III. PROPOSED EMBEDDING PHASE

The clear ideologies about the steganography are stated in the work through the proposed philosophy. In the proposed steganography methods are consisting of two phases like Embedding Phase and Extraction Phase. The embedding phase hides the secret message that is intended to the receiver. Masking, filtration and transformation are leading factors in steganography. The Phase coding, echo hiding coding and audio coding using the LSB coding for maintain security issues. Steganography system has got two methods one is public key steganography and pure steganography which is not under the technique of cipher called as stego- key. This method is not that much be appreciated because of simple assumptions that no one can have knowledge about the keys . The cryptography and steganography was integrated in order to improve the security. In the approach presented in the paper [11], the combination of steganography and cryptography is further strengthened by including a compression technique before using the encryption process. The two level secured edge based image steganographic approach is proposed to hide secret information of variable size in a cover image [12].

The sensitive data is the beneficial for security reasons in steganography and hiding the password or keys into another file is the great burden and detecting the same is also so hectic in nature. Browsers cannot detect the data from the image casually but long standing work is needed to find the text which is embedded inside the image. The pixels inside the image should be changed, so that others and intruders cannot identify the text which is inside the image.

In the phase, it ensures security to the message, increases capacity, decreases imperceptibility and provide robustness [7]. In the phase, the sender creates the stegno image in three stages and the process as follows. ENCRYPTION: The process randomizes the secret message and provides security to the message. The secret message is encrypted using Transposition cipher. It is a technique in which the plaintext is arranged in a matrix format and permuted to get the cipher text. The text in the transposition matrix is obtained by the XOR operation with the key produced through hyper elliptic curve cryptography [3]. Reverse permutation gets back the required plain text at the other end whom the image is delivered. Even if the intruder finds the message, the third party cannot understand the message because of encryption. COMPRESSION Phase: To increase the occupational capacity in the encrypted message should be compressed using a lossless compression technique. Huffman Coding technique was employed on the encrypted text. It is an entropy encoding algorithm used for lossless data compression [10]. Huffman algorithm uses characters with fixed length as input and obtains output bits of different length. The primary aim of the Huffman coding is assigned to small code words to the characters with a higher occurrence and long code words to the character with lesser occurrence. It is similar to Morse code concept. A Huffman code is designed by merging together with two least occurring characters and repeated until one character is left. A code word tree is obtained and the Huffman tree is generated by labeling the code tree [4]. EMBEDDING PHASE: The compressed text is embedded into the least significant bit of each pixel following the Knight's Tour algorithm [2]. A knight's tour is an 'L' shaped pattern of a knight on a chessboard and traversing each block only one time. It is said to be closed, If the traversal completes on a block for one traversal of the knight, else it is open. Simple Least significant bit (LSB) insertion is a conventional method of embedding data in the cover file. Backtracking can be done to trace the Knight Tour path. One such solution for 8 X 8 chessboards is shown in the Fig. 1.

1	45	31	50	33	16	63	18
30	51	46	3	62	19	14	35
47	2	49	32	15	34	17	64
52	29	4	45	20	61	36	13
5	44	25	56	9	40	21	60
28	53	8	41	24	57	12	37
43	6	55	26	39	10	59	22
54	27	42	7	58	23	38	11
1	45	31	50	33	16	63	18
30	51	46	3	62	19	14	35
47	2	49	32	15	34	17	64
52	29	4	45	20	61	36	13
5	44	25	56	9	40	21	60
28	53	8	41	24	57	12	37
43	6	55	26	39	10	59	22
54	27	42	7	58	23	38	11

Fig. 1. 8 X 8 Chessboards.

A. Extraction Phase

The extraction phase is done at the receiver end. First, the data is extracted from the cover image. The obtained secret message is decompressed. After decompression cipher text is obtained. Using the key the receiver decrypts the cipher text and extracts the secret message. In the way, the secret message is made secured. Even if the intruder extracts the message it is impossible to understand the message as it is encrypted and compressed before the embedded process.

IV. RESULTS AND DISCUSSIONS

The proposed method provides security, imperceptibility, capacity and robustness characteristics to the secret image. Compared to a simple Least Significant Bit Steganography, the proposed method is analyzed with the above-said characteristics. The method provides security by using Encryption techniques which randomize the secret message. In simple LSB the secret message is embedded in the LSB of consecutive pixels. Whereas in the enhanced LSB secret message is embedded in LSB based on the knight tour pattern. Thus by provides the additional security to the message. By compressing the text, the occupational capacity is increased. So that large text can be embedded into the image. Thus the key characteristics were analyzed and the proposed method characterized the advantages of the result generated.

For the steganalyst find difficult in identifying the technique that adapted inside the research work because of the style of movement of the horse in the chessboard. Covering image in the steganography is the different model and finding the transformed text pixel is the hectic task for the hackers and identity the text structure is also a great task. For the researchers this is new eye open to do the same with different effect using cryptography.

In the framework of the stegnography alter the images should be in the passive way. The straight forward simple method is LSB transformation approach. In the public domain many LSB methodologies are available and in our work we proposed the different techniques that may not affect the image and no one can understand about the tunneling text inside the image.

V. CONCLUSION

In the recent past steganography, applied methodologies were widely used by many researchers. In the work, we proposed the new methodology called Horse tour in the chessboard and hide the text message characters in the rightmost side of the bit. The reason behind it is all simple that it will not make any significant change in the image. In Bitwise pattern, the rightmost position called as Least significant bit. The image looks the same but inside the image, the huge message was embedded. The position of the bit can be identified by the receiver using the horse move style in the chessboard. Every starting position should be calculated and through which the ending position can be identified and that it will be the place to store the character is the newer method adapted in the paperwork. In the extraction phase the receiver having the software to locate the position of the hidden character. Using different styles of the move which is available in the chessboard can be used to embed the characters for secured transmission in the unsecured network.

REFERENCES

[1]. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing,* **90**(3), 727-752.

[2]. Parberry, I. (1997). An efficient algorithm for the Knight's tour problem. *Discrete Applied Mathematics,* **73**(3): 251-260.

[3]. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., & Vercauteren, F. (2005). Handbook of elliptic and hyperelliptic curve cryptography. Chapman and Hall/CRC.

[4]. Kailasananathan, C., Safavi-Naini, R., & Ogunbona, P. (2000). Secure compression using adaptive Huffman coding.

[5]. Chen, Y.Z., Han, Z., Li, S.P., Lu, C.H., & Yao, X.H. (2010, October). An adaptive steganography algorithm based on block sensitivity vectors using HVS features. *In 2010 3rd International Congress on Image and Signal Processing* (Vol. **3**, pp. 1151-1155). IEEE.

[6]. Potdar, V. M., Han, S., & Chang, E. (2005). Fingerprinted secret sharing steganography for robustness against image cropping attacks. In INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. (pp. 717-724). IEEE

[7]. Shirali-Shahreza, M.H., & Shirali-Shahreza, M. (2006). A new approach to Persian/Arabic text steganography. In 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR'06) (pp. 310-315). IEEE.

[8]. Lin, E. T., & Delp, E. J. (1999). A review of data hiding in digital images. In PICS, Vol. **299**, pp. 274-278.

[9]. Chang, C. C., Lin, C. Y., & Wang, Y.Z. (2006). New image steganographic methods using run-length approach. *Information Sciences*, **176**(22), 3393-3408.

[10].Hwang, R. J., Shih, T. K., Kao, C. H., & Chang, T. M. (2001). Lossy compression tolerant steganography. In International Conference Human Society@ Internet (pp. 427-435). Springer, Berlin, Heidelberg.

[11]. Manikandan, G., Kamarasan, M., Rajendiran, P., & Manikandan, R. (2011). A hybrid approach for security enhancement by modified crypto-stegno scheme. *European Journal of Scientific Research*, **60**(2), 224-230.

[12]. Jena, K.K., Mishra, S., Mishra, S. and Bhoi, S.K. (2019). An Edge based Steganographic Approach using a two Level Security Scheme for Digital Image Processing and Analysis, *International Journal on Emerging Technologies*, **10**(2): 29-38

How to cite this article: Rajendiran, P., Sekar, K.R., Ramesh, C. and Manikandan, R. (2019). Novel Steganography Methodology Applied in Transposition Cipher for Hiding Text message. *International Journal on Emerging Technologies*, **10**(2): 156-158.