International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-06, Issue-01, Apr 2020

A literature Review of Cryptography on RC4 Stream Cipher and Hash-LSB Steganography

[1]Yogini Eknath Lamgaonkar, [2]Melina Maria Afonso

[1]Student, [2]Assistant professor, Department of CSE, Goa College of Engineering, Goa, India.

Abstract--In the modern world with the emergence of technology, the entire network includes the digital data that adds new dimensions as to how data can be exchanged effectively and safely in real time from one part of the world to another. Such new opportunities are followed by obstacles such as keeping information confidential and secret or data that is a lively area to explore. It is necessary to transform the information into cryptic form to safely transfer the information from intruders, so that the information is concealed from the intruders.

Researchers have always found it fascinating to establish safe techniques that would allow the data to reach from the sender without exposing it to third parties. Therefore several techniques have been developed to transfer data securely and steganography is one of them. In this paper, we review numerous research papers on different techniques of encryption and steganography. This paper contains details about the RC4 encryption algorithm, and how steganography and encryption methods are used. The cryptography and steganography techniques ensure the security of the data.

Keywords – cryptography, steganography, public key encryption, symmetric key encryption, RC4 algorithm, HASH-LSB

I. INTRODUCTION

In the recent years network security has been crucial factor in communicating and transferring data from one network to another. Steganography & Cryptography are techniques used for network security. Steganography is an encryption technique that can be used in combination with cryptography to ensure extra protection for sensitive data and to secure it against intruders. Steganography techniques can be applied to images, an audio file or a video file.

Cryptography transforms data into an unreadable format to prevent an unauthorized user from accessing it, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thereby preventing data protection.

II. CRYPTOGRAPHY

Cryptography is a method or a tool that is used to protect information being communicated through the use of codes so that only those for whom the information is intended can read and process the confidential data.

Cryptographic algorithms are divided into symmetric key algorithm and asymmetric key algorithm or public key algorithm.

Public key encryption is a method of encryption in which the message is encrypted with a public key of a receiver. Only the intended recipient may use private key to decrypt the information.

Symmetric key encryption is also called as private key encryption; in this technique, encryption and decryption process is achieved using a single key. Both parties share the same key; that is the sender, and the receiver. If the sender codes the message with one key, the recipient must decrypt the message with the same key.

III. STEGANOGRAPHY

Steganography is a method where the detail is hidden. Therefore, when we use steganography, hidden knowledge is often transmitted and we seek to transmit this knowledge only to the intended recipient and not readable even if it is found by unintended individual. The sender hides a message into a cover file such as image, audio, video and attempts to conceal the message's presence. The receiver gets this cover file later, and detects and uncovers the hidden message. Steganography means writing by cover. It's history is old and its usage was inspired by different practices of hiding writing for e.g. making a tattoo on a messenger head after shaving his hair and letting his hair grow again and then send it to the recipient where his hair was shaved there to get the message; writing on a wooden tablet and then covering it with wax; other techniques such as invisible ink were often used for writing between microdots and using the arrangement of characters.

 DOI : 10.35291/2454-9150.2020.0308

Steganography Types

1) Text Steganography
   Text steganography consists of hiding information inside the text message. In this the secret data is hidden behind every n^{th} letter of any text file word.
2) Image Steganography
   Hiding is done by considering the cover object that is image; the pixel intensities are used to hide the data.
3) Audio Steganography
   It is a technique in which data is hidden in audio files.
4) Video Steganography
   Video steganography requires hiding files or data of some kind in digital video format. This video is used as shielding carrier for the data.

IV. LITERATURE SURVEY

Paper 1:RC4 Technique in Visual Cryptography RGB Image Encryption

This paper presents the encryption of the RGB image in visual cryptography. RC4 is the encryption algorithm which offers the right method to cover up or manipulate the content of the picture. RC4 encryption algorithm has three levels option to allow us to select which layer is encrypted [1]. The approach mentioned in this paper provides high security.

Paper 2: An Efficient Image cryptography using Hash-LSB steganography with RC4 and Pixel shuffling Encryption Algorithms

The author abood et al. [2] proposed a cryptographic method along with steganography. The RC4 and pixel shuffling encryption algorithms are used along with Hash LSB stenography technique to encrypt the secret image. The proposed methodology enhanced steganography technique by concealing data in an image which makes stated algorithm more effective and secure and the author also stated that decrypted secret image without affecting the quality of images in terms of MSE, Security quality and PSNR.

Paper 3: New Approaches to encrypt and decrypt data in image using cryptography and steganography Algorithm

The author has clarified a proposed technique for Cryptography and steganography to provide security in network setting. The author focuses primarily on designing a framework that provides additional security features. Hash Least Significant Bit (H-LSB) along with affine cipher encoding algorithm has been proposed to provide data in a network environment with protection and confidentiality [3]. Hash LSB technique is 3-3-2 LSB technique used in this article. The proposed framework has potential to provide improved protection and a simple way to encrypt and decrypt hidden messages without sacrificing the picture quality visible to the naked eye. Therefore this method is very efficient and successful in hiding the information within the image.

Paper 4: Hash based LSB technique for video steganography (HLSB)

This paper proposed a hash based LSB techniques for videos in the spatial domain. Hash LSB technique is 3-3-2 LSB technique used in this article. Eight bits of the hidden data information are split into 3, 3, 2 bit format and inserted respectively in the RGB pixel values of the cover frames. To pick the location of insert bits in the cover image LSB frames a hash function is used. The proposed methodology is compared with existing LSB Steganography techniques and the results were encouraging [4].

Paper 5: A Novel Hash based LSB (2-3-3) image steganography in spatial domain

A hash based LSB Techniques in spatial domain is proposed in this paper. The HLSB technique used in this article is 2-3-3 LSB technique. Eight secret information bits are divided into 2, 3, 3 bit format and embedded respectively within the RGB pixel values of the cover image frames. For selecting the insertion location in LSB bits of the cover image, a hash function is used. They compared the technique of HLSB 2-3-3 and 3-3-2 and concluded that the stenographic technique HLSB 2-3-3 is better than the technique of HLSB 3-3-2 in terms of MSE and PSNR, NAE, SSIM values [5].

Paper 6: RC4 Encryption-A Literature Survey

This paper presents a survey showing how the RC4 stream cipher algorithm is cryptanalysis. The author has summarized numerous RC4 algorithm vulnerabilities followed by the latest proposed improvements available in the literature. Innovative research efforts are required to develop stable and secure RC4 algorithm that can remove the RC4 weaknesses [6].

Paper 7: Digital Image confidentiality depends upon Arnold transformation and RC4 algorithm

This paper addresses confidentiality and image protection that relies on spatial domain transformation (Arnold transformation) as well as one stream cipher algorithm (RC4). This paper introduces three phases; the first phase is the design and implementation of digital image scrambling based on best iteration using Arnold transformation. In the second phase, the design and implementation of the RC4 stream cipher for colour image encryption and in the third step author have implemented Arnold and RC4 algorithms based on best iteration that Arnold transforms to scramble image and then use the

 DOI : 10.35291/2454-9150.2020.0308

RC4 algorithm to encrypt it. The author also provided a detailed comparison of all the techniques in terms of coefficient of correlation and quality factor for safety. Using blum blum shub (BBS) random bit generator algorithm the input key to the RC4 algorithm is generated. All phases are executed using Matlab[7].

Paper 8: Digital Colour Image Encryption using RC4 stream cipher and chaotic logistic map

This paper presents novel stable and secure image encryption algorithm, based on RC 4 stream cipher and map of chaotic logistics [8]. The algorithm suggested function as follows:
(i) Converting an external key to an initial value,
(ii) Generating a key stream using a chaotic logistic map function,
(iii) Processing a permutation and the output is then XOR-ed with a digital image byte stream.

The results of the experiments show that the proposed algorithm is
(i) The encrypted image which is cipher image cannot be visually detected by humans
(ii) The statistical similarity between the input-image and cipher-image can be eliminated,
(iii) The algorithm can be influenced by minor key changes,
(iv) The size of input image and encrypted image cannot be modified.

Paper 9: Evaluation of the RC4 algorithm for Data Encryption

Mousa et al. [9] study the RC4 parameters and showed that the speed of encoding and decoding time is directly related to an enciphered key length and size of the data file, if the data is large enough. Data type is also important as image data needs a longer processing time than text or sound data due mainly to the larger file size. This relationship has been translated into equations to model these relationships and can therefore be used to predict the RC4's output under various conditions.

Table 1. Comparison Table

Paper Name	Algorithm/Technique used	Merits	Demerits
RC4 Technique in Visual Cryptography RGB Image Encryption	RC4	Algorithm provides high security	After decryption, it reduces the file size
An Efficient Image cryptography using Hash-LSB steganography with RC4 and Pixel shuffling Encryption Algorithms	RC4, Pixel shuffling, HLSB	Enhances data security and also becomes more effective and powerful mechanism Does not affect the quality of images(MSE,SQ and PSNR)	Hash LSB (3,3,2) technique does not give better results in terms of MSE and PSNR
New Approaches to encrypt and decrypt data in image using cryptography and steganography Algorithm	Affine cipher, HLSB	Provides better data security, accuracy and confidentiality	Affine cipher is a simple algorithm Brute force attack
Hash based LSB technique for video steganography (HLSB)	HLSB	Technique can be work for all formats with minor modifications For flash video files does not need any modifications to technique	Decompression need to be performed for compressed videos like MPEG.
A Novel Hash based LSB (2-3-3) image steganography in spatial domain	HLSB(2,3,3) and HLSB(3,3,2)	HLSB(2,3,3) provides better result compared to HLSB(3,3,2) with reference to MSE, NAE PSNR and SSIM	Easy to decrypt Less secure
RC4 Encryption-A Literature Survey	RC4	Simple and Robust	Biased bytes, key recovery attacks on WPA and key collisions in key stream
0Digital Image confidentiality depends upon Arnold transformation and RC4 algorithm	Arnold Transformation, RC4	Arnold transformation to scramble digital images and later to encrypt using RC4 provides high security performance	Security quality factors are zero in Arnold transformation
Digital Color Image Encryption using RC4 stream cipher and chaotic logistic map	RC4, chaotic logistic map	Cipher image cannot be visually seen by human eye No changes in file size between plain-image and cipher-image(lossless encryption)	Sensitive to external key value
Evaluation of the RC4 algorithm for Data Encryption	RC4	Simple and robust Encryption and decryption time is based on the key length and data size	Image data requires large time as compared to text or sound data.

 DOI : 10.35291/2454-9150.2020.0308

IV. CONCLUSION

In this paper, we present literature survey review on various techniques of image encryption and steganography. Different encryption and steganography techniques are used for converting input image into cipher image. Steganography is used to enhance the security of the data. The encryption key will be hidden into cipher image without affecting it. This will reduce the cost of key distribution and also save time involved in sending keys between the two parties. Since RC4 has vulnerability it is combined with HLSB Technique to make it more secure. It is also concluded that along with RC4 algorithm it is better to use Hash LSB 3-3-2 instead of 2-3-3 because it gives better results in terms of quality measures MSE and PSNR.

REFERENCES

[1] Siahaan, Andysah Putera Utama. (2016). RC4 Technique in Visual Cryptography RGB Image Encryption. International Journal of Computer Science and Engineering. 3. 2348-8387. 10.14445/23488387/IJCSE-V3I7P101.

[2]May H. Abood "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms", IEEE, July 2017

[3] Ako Muhammad Abdullah and Roza Hikmat Hama Aziz "New Approaches to encrypt and decrypt data in image using cryptography and steganography Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 143 – No.4, June 2016.

[4] P. R. Deshmukh and B. Rahangdale, "Hash Based Least Significant Bit Technique For Video Steganography", Int. Journal of Engineering Research and Applications, vol. 4, no. 1, pp. 44–49, January 2014.

[5] G.R.Manjula and AjitDanti "A NOVEL HASH BASED LEAST SIGNIFICANT BIT (2-3-3) IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015

[6] Poonam Jindal and Brahmjit Singh "RC4 Encryption-A Literature Survey" International Conference on Information and Communication Technologies.(Elsevier) (ICICT 2014)

[7] K. Hamdnaalla, A. Wahaballa, and O. Wahballa, "Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms",International Journal of Video & Image Processing and Network Security, vol.13, no. 04,August 2013.

[8] N. G. A. P. H. Saptarini, Y. A. Sir, "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map",Information Systems International Conference ,December, pp. 2–4, December 2013.

[9] A. Mousa and A. Hamad, "Evaluation of the RC4 Algorithm for Data Encryption," no. 1, pp. 44–56, June2006.

[10]https://www.vocal.com/cryptography/rc4-encryption-algoritm/

[11]https://sandilands.info/sgordon/teaching/reports/rc4-example.pdf

[12] B. H. Kamble, "Robustness of RC4 against Differential attack" ,International Journal of computer science and application, vol. 1, no. 4, pp. 661–665, June 2012.

 DOI : 10.35291/2454-9150.2020.0308