IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Data Transmission Using CRYPTO-STEGO Approach

Monika* Dr. Gundeep Tanwar**

*(Student of Master of Technology in Computer Science & Engineering, Rao Pahlad Singh College of Engineering & Technology, Balana(Mahendergarh)

**(Assistant Professor in Department of Computer Science & Engineering, Rao Pahlad Singh College of Engineering & Technology, Balana (Mahendragarh)

Abstract:

Cryptography is a process to secure data transmission using Encryption and decryption over the internet. This paper proposed concept to enhance the data encryption and decryption security by using combination of both Cryptography and Steganography techniques. In Cryptography there is used Rivest-Shamir-Adleman (RSA) Algorithm. In Steganography there is used Image Steganography for hiding the data. Through using combination of both cryptography and steganography security of data is increased which is also known as CRYPTO-STEGO Approach. This satisfies all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. And data can be maintained more securely. There can used RSA for encryption of data and Steganography approach to hide the data in an image so that data can not be accessed by anybody in network and only sender and receiver can retrieve the data from message file. [1]

Keywords — RSA Algorithm, Cryptography, Steganography.

I. INTRODUCTION

In Today's world, Data security has become basic issue. Steganography and cryptography are two popular ways of sending the information in a secret way. One method used to hide the existence of the message, and the other will distort the message itself. Through this research paper mainly focus to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like cryptography and steganography.

Currently, most of the departments in government, military communication, financial institution, medical imaging, and private business greatly deal with data that are in the form of images. So, security of digital images has become most important. [2]

II. CRYPTOGRAPHY

The basic idea of cryptography is to encrypt the information or data in such a way that an unauthorised person cannot access it. Cryptography is mainly used to send data via an unsecured channel, such as internet, or used to ensure that unauthorised persons do not comprehend what they are looking at in a case where they have accessed the information.[3]

In Cryptography, the original message is known as plaintext. And the process to convert the original message into another form which can not be understood by third person is known as encryption. The encrypted message is known as ciphertext. This all done through some encryption algorithm using some encryption key.

Its reverse process is known as decryption which will convert the cipher text into plain text(Original message) through some decryption algorithm using decryption key.

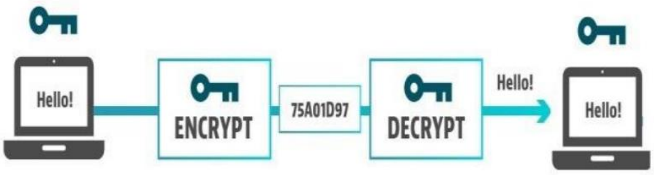


Fig. 1. Cryptography concept

III. STEGANOGRAPHY

It is the process of hiding and communicating data through some reliable carriers in attempt to hide the existence of the data. While sending data information from sender to receiver, using Steganography information will be hidden in such a way that others cannot distort the message by itself. The secret information is inserted into the cover media by the stego system which will be encoder by using certain algorithm. A secret message can be either plaintext, an image, ciphertext, or anything which can be represented in form of a bitstream. after the secret data 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. Steganography is mainly used for image files or audio files.[4]

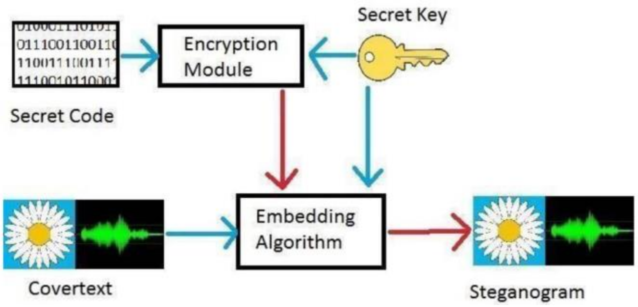


Fig. 2. Steganography process

Various ways of Steganography

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.

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. [5]

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 file for examples Phase Coding, LSB.

Video Files

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

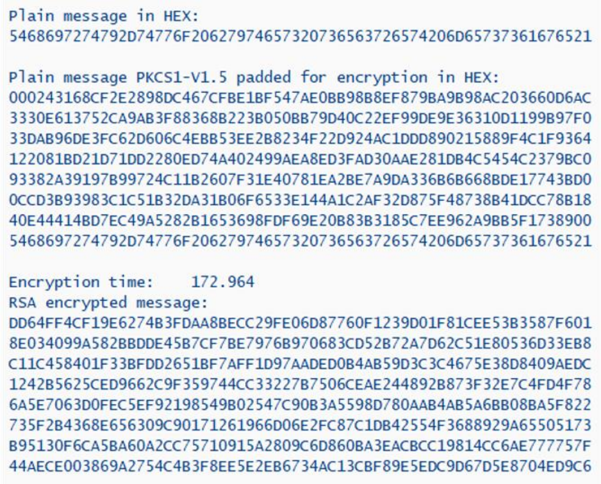
IV. PROPOSED CRYPTO - STEGO

There proposed new approach of encryption and decryption. In this approach keyless encryption and decryption. This method is very light weighted and secure as there is no such separate key is required. The key to decrypt that message is itself encrypted within the message. In the traditional key encryption method if the key is somehow stolen by the third person, then the data can be misused. Therefore, the proposed system is more secure because there is no involvement of transmission secret key.

Proposed encryption in two ways-

1. **Text to text cryptography** (RSA Algorithm)

In proposed system the encryption in first phase depends upon the length of the secret message. Each letter is first converted into its Unicode value. This Unicode value is added into the total length of the message. The result of this is considered as a Unicode and the symbol associated with that Unicode is used for that letter. By this method every time the encryption letter changes with the change in the length of the message. For decrypting the message this process is used in reverse manner. The Unicode of each letters is decreased by the total length of the message and then it is converted into the actual letter.[6]



```
Plain message in HEX:
5468697274792D74776F206279746573207365637265742064D65737361676521

Plain message PKCS1-V1.5 padded for encryption in HEX:
000243168CF2E2898DC467CFBE1BF547AE0BB98B8EF879BA9B98AC203660D6AC
3330E613752CA9AB3F88368B223B050BB79D40C22EF99DE9E36310D1199B97F0
33DAB96DE3FC62D606C4EBB53EE2B8234F22D924AC1DDD890215889F4C1F9364
122081BD21D71DD2280ED74A402499AEA8ED3FAD30AAE281DB4C5454C2379BC0
93382A39197B99724C11B2607F31E40781EA2BE7A9DA336B6B668BDE17743BD0
0CCD3B93983C1C51B32DA31B06F6533E144A1C2AF32D875F48738B41DCC78B18
40E44414BD7EC49A5282B1653698FDF69E20B83B3185C7EE962A9BB5F1738900
5468697274792D74776F206279746573207365637265742064D65737361676521

Encryption time:    172.964
RSA encrypted message:
DD64FF4CF19E6274B3FDAA8BECC29FE06D87760F1239D01F81CEE53B3587F601
8E034099A582BBDDE45B7CF7BE7976B970683CD52B72A7D62C51E80536D33EB8
C11C458401F33BFDD2651BF7AFF1D97AADED0B4AB59D3C3C4675E38D8409AEDC
1242B5625CED9662C9F359744CC33227B7506CEAE244892B873F32E7C4FD4F78
6A5E7063D0FEC5EF92198549B02547C90B3A5598D780AAB4AB5A6BB08BA5F822
735F2B4368E656309C90171261966D06E2FC87C1DB42554F3688929A65505173
B95130F6CA5BA60A2CC75710915A2809C6D860BA3EACBCC19814CC6AE777757F
44AECE003869A2754C4B3F8EE5E2EB6734AC13CBF89E5EDC9D67D5E8704ED9C6
```

Fig. 3 RSA Encryption

2. **Text to image steganography**

In the first phase the text is encrypted into another text. In this phase, the system will encrypt that text into an image. For this the system uses a sample image to hide the text behind it. First image is converted into its bitmap where each pixel represents its RBG value. The text is treated as a pixel so every letter in the text acts as one pixel. These pixels are plotted in the sample image by replacing some of its pixels. For choosing which pixels to be replaced are decided by using the GCD logic (Whiting). In this the GCD of the length and width of the image is found and it stored in n. After this, every nth pixel of the image is used for the replacement.[7] When the replacement is done a new image is formed and this image is used for the transmission. While decrypting the image again GCD is found and the pixels on that result are converted back into the text. [8]

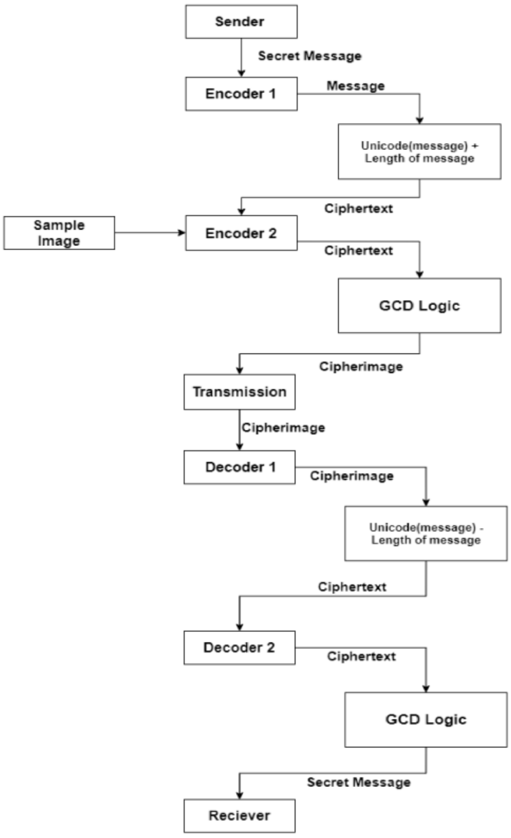


Fig. 3. **crypto-stego workflow**

V. Future Scope

The main aim of crypto-steganography system is to hide the message into image. It will work for any size of data. In future if there need to extend the system for providing security the same algorithm will work effectively. There need to first encrypt the message and then encrypted code which is cipher text is hidden in the image using LSB substitution with GCD logic. For the enhancement of this system we can use RGB substitution, AES, Random key dependent algorithms in combination; to provide security for the preservation of documents.[9]

VI. CONCLUSIONS

Through cryptography or steganography, there can provide security of data with secrete key. But through this paper, proposed an new approach with combination of both, cryptography and steganography with keyless transmission of data which helps to improve the security at greater extent. In this approach the cryptographic method involves a different technique which uses message length and its Unicode value for encryption and similarly steganographic method also uses different technique which uses format like bmp, jpg etc. We have tested the system on different size of images from 250 x 150 to350 x 250. We found the result in such a way that the data hidden in the cover image does not affect the original size of the image. More than 90% of the image is preserved and only the intended receiver knows its existence.[10]

ACKNOWLEDGMENT

It is a matter of great pleasure for me to submit this report on the Research Paper entitled **“Secure Data Transmission Using CRYPTO-STEGO Approach”**, as a part of curriculum for the award of “Master of Technology” in Computer Science & Engineering, Rao Pahlad Singh College of Engineering & Technology, Balana (Mahendragarh). I would like to express my sincere gratitude to the faculty of Computer Science & Engineering Department, Rao Pahlad Singh College of Engineering & Technology, Balana (Mahendragarh) for the constant encouragement, expert advice, guidance, devotion and timely suggestions which helped me at every stage of this work. I would also like to thank to all my family members and friends who have helped me in one way or another.

Author’s Contributions

All authors equally contributed in this work.

REFERENCES

[1]. Ramalingam, M., Nor Ashid Mat Isa and Puviarasi. (2020), “A secured data hiding using affine transformation in video steganography", 3rd International conference on computing and network communication 2019, Procedia Computer Science 171 (2020) 1147–1156

[2]. Varalakshmi, R. (2020), "Digital steganography for preventing cybercrime using artificial intelligence technology", Journal of critical reviews ISSN - 2394- 5125, vol 7, issue 6.

[3]. Bhagat, Jayti, Gupta, P. and Kohli, N. (2018), "Image Steganography Using Improved Algorithms to Enhance Security and Payload of Traditional LSB Substitution." 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE.

[4]. Zaware, S. (2019), “Secure Digital Document Generation Using QR Code” Journal of Adv Research in Dynamical & Control Systems, ISSN: 1943-023X, Vol. 11, Special Issue-08, and 3241-3249

[5]. Mehboob, B. and Faruqui, R. A. (2008), "A stegnography implementation," 2008 International Symposium on Biometrics and Security Technologies, Islamabad, pp. 1-5

[6]. Darbani, A., AlyanNezhadi, M.M. and Forghani, M. (2019), A New Steganography Method for Embedding Message in JPEG Images, 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), Tehran, Iran, pp. 617-621

[7]. Gupta, R. and Singh, T. P. (2014), "New proposed practice for secure image combing cryptography steganography and watermarking based on various parameters," 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, pp. 475-479

[8]. Duan, X., Guo, D., Liu, N., li, B., Gou, M., and Qin, C. (2020), “A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network", IEEE Access publication February 4, 2020

[9]. Kanojia, Pallavi & Choudhary, V. (2019). LSB Based Image Steganography With The Aid of Secret Key and Enhance its Capacity via Reducing Bit String Length. 257-262. 10.1109/ICECA.2019.8821917

[10].Ramalingam, M., Nor Ashid Mat Isa and Puviarasi. (2020), “A secured data hiding using affine transformation in video steganography", 3rd International conference on computing and network communication 2019, Procedia Computer Science 171 (2020) 1147–1156