RESEARCH ARTICLE OPEN ACCESS

Steganography and Cryptography An Art of Hiding Data

Tahamina Yesmin
Department of Computer Gaming and Mobile App Development
Haldia Institute of Management, Haldia, Purba
Medinipur – India

ABSTRACT
Transmission of data through internet has become very common now a day so, it is important to have secure communication over internet. Cryptography and Steganography are two important methods for providing secure communication. We know cryptography and steganography are two methods used for data protection. The cryptography distorts the data and steganography hides the existence of data. But both of them have their own vulnerabilities, in this paper we are focused to combine cryptography and steganography in various ways to enhance the security of data.

Keywords:- Cryptography, Steganography, Encryption, Decryption, Advance encryption standard (AES), Data Security, Information Hiding, Information Security, Data hiding.

I. INTRODUCTION

1. The cryptography and steganography are two widely used techniques for confidentiality of data exchange. Cryptography is used to cipher information and steganography is used to hide the existence of data communication. To manipulate or hide the existence of a message, cryptography and steganography are two best techniques. Cryptography scrambles the message so that the message cannot be understood. And steganography hides the existence of the message so that the message is not visible. And combination of both Cryptography and steganography makes the communication more confidential and secure. A cryptographic key was used to decode the message that was known only by the authorized persons. The limitation of cryptography was that other person came to know that the message had a hidden text in it and so the probability of message being decoded by other person increased. To overcome this limitation the technique of steganography was introduced.

Information transmission through internet may include sensitive personal data which may be intercepted. Also, there are many applications on the internet and many web sites require the users to fill forms that include sensitive personal information such as telephone numbers, addresses, and credit card information. So, the users may need private and secure communications for many reasons such as protect their confidential information from hackers during it passed over an open channel, so the confidentiality and data integrity are required to protect against unauthorized access and use. Cryptography and steganography are the common methods to secure communications [1].

One of the reasons why attackers become successful in intrusion is that they have an opportunity to read and understand most information from system. The most important motive for attacker to benefit from intrusion is value of confidential data he can obtain by attacking the system. Hackers may expose the data, alter it, distort it or employ it for more difficult attacks. The solution for this problem has led to the development of cryptography and steganography. By combining cryptography and steganography in one system we can ensure enhanced security [2].

We can use steganography over the cryptography, these are very closely related to each other. The use of cryptography as a way to secure the hidden message mainly addresses the security requirement in the Information-Hiding system. For the purpose of steganography, symmetric encryption is followed. The symmetric encryption is a method of encryption that uses the same key to encrypt and decrypt a message.
If one person encrypts and decrypts data, that person must keep the key secret. If the data is transmitted between parties, each party must agree on a shared secret key and find a secure method to exchange the key. The security of encrypted data depends on the secrecy of the key.

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 [3].
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. [4].

The studies that attack the encrypted message and detect the hidden messages are called as Cryptanalysis and Steganalysis. So, we should apply those algorithms that are hard to crack.

II. RELATED WORKS

In [5] authors proposed a method that increase the security of data transfer by combining cryptography and steganography. Mp3 file is taken as the cover media and the secret message is encrypted using AES algorithm using a key that has been processed by MD5 hash function. The secret message was inserted in the homogeneous frame in mp3 files with addition of a key code. The MD5 algorithm is a widely used cryptographic hash function used to verify data integrity.

In [6] authors presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) environment. They proposed a technique that employs an integrated approach of steganography and cryptography during data transfer between IoT device & home server and home server & cloud server. The sensed data from IoT device is encrypted and embedded in the cover image along with message digest of sensed data and send to the home server for authentication purpose. At the home server the embedded message digests and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is carried out between home server and cloud server.

In [7] authors give an example where, Steganography can be used in a lot of useful applications. For example copyright control of materials, to enhance the robustness of an image search engines and smart identity cards where the details of individuals are embedded in their photographs. Other applications include video-audio synchronization, TV broadcasting, TCP/IP packets where a unique ID is embedded in an image to analyses the network traffic of particular users.

[8] In this paper the author states that steganography is a technique which hides the data in such a way that it is not visible to user. Steganography has divided into many types like Audio, Video, Text, Image. In case of image steganography data is hidden behind the image. In this cover image is used to hide the data. The image obtained after embedding the data is known as stego image. Various methods used for steganography are like LSB, Transform Domain, DFT and many more. All the techniques have some advantages and disadvantages. In this paper enhanced LSB technique is developed by the author who overcomes the limitations of other techniques. LSB technique for color images by embedding the information into three planes of RGB image in a way that enhances the quality of image and achieves high embedding capacity. The PSNR value of the proposed technique is better than previous steganography methods.

In [9], 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.

The paper at [10] 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 [11], 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.

2.1. Proposed System:

The point of proposed plan is to make an increasingly secure and hearty strategy for data trade with the goal that secret and private information must be ensured against assaults and unlawful access. To arrange in accomplish the necessary vigor and security cryptography and steganography is joined. Picture is taken as a spread mechanism for steganography and RSA calculation is utilized for encryption.

In this proposed technique our progressed LSB bit control strategy is utilized for inserting the message in the picture document and the message is itself encoded utilizing the current RSA encryption strategy. For installing the content in picture document initially both the content and picture record are changed over into twofold proportional and afterward content is scrambled utilizing RSA. The scrambled content is then installed into the picture record utilizing our progressed LSB calculation.

2.2. *Cryptography*:

Cryptography is one of the conventional techniques used to ensure the protection of correspondence between parties. This strategy is the specialty of mystery composing, which is utilized to encode the plaintext with a key into ciphertext to be moved between parties on a shaky channel. Utilizing a substantial key, the ciphertext can be unscrambled to the first plaintext. Without the learning of the key, it's not possible for anyone to recover the plaintext. Cryptography assumes a basic job in numerous variables required for secure correspondence over a shaky channel, similar to: classification, protection, non-renouncement, key trade, and confirmation. Figure 1 shows the cryptography system [12].

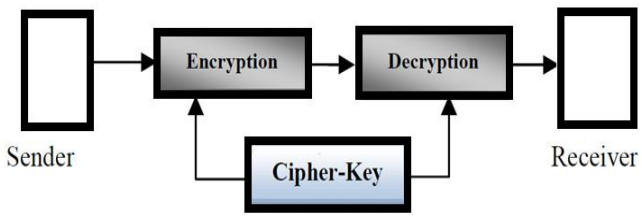

Fig. 1

There are a few different ways of characterizing cryptographic calculations. The three sorts of calculations are:
(1) Secret key Cryptography: Uses a single key for both encryption and decryption
(2) Public Key Cryptography: Uses one key for encryption and another for decryption.
(3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

2.3. *Secret Key Cryptography:*

The method of Secret key encryption can likewise be known as the symmetric-key, shared key, single-key, and in the end private-key encryption. The procedure of private key uses for all sides' encryption and decoding mystery information. The first data or plaintext is scrambled with a key by the sender side likewise the comparatively key is utilized by the collector to decode a message to get the plaintext. The key will be known distinctly by a people who are approved to the encryption/unscrambling [13].

Nonetheless, the system bears the great security for transmission however there is a trouble with the appropriation of the key. In the event that one took or investigate the key he can get entire information with no trouble. A case of Symmetric-Key is DES Algorithm [13].

2.4. *Public Key Cryptography*

We can call this procedure as deviated cryptosystem or open key cryptosystem, this system utilize two keys which are scientifically related, use independently for scrambling and unscrambling the data.

In this method, when we utilize the private key, there are no potential outcomes to get the information or basically find the other key. All keys are required for the strategy to run. The key utilized for encryption is put away open along these lines its called open key, and the unscrambling key is put away mystery and called private key. A case of Asymmetric-Key Algorithms is RSA [12].

2.5. *RSA Algorithm:*

RSA is one of the most punctual open key cryptosystems and it is generally utilized for verifying information transmission. RSA was first depicted in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Here encryption key is open and decoding key is private, it stayed quiet. RSA depends on factorizing two enormous prime numbers. People in general and the private key-

age calculation is the most unpredictable piece of RSA cryptography. We can create two huge prime numbers, x and y, utilizing the Rabin-Miller primality test calculation. A modulus is determined by increasing x and y. This number is utilized by both people in general and private keys and gives the connection between them. Its length is known as the key length.

RSA calculation method can be shown in brief as follows:

1. Pick two huge prime no. p and q.
2. Figure N=p*q
3. Figure f (z) = (p-1)*(q-1) Find an irregular number e fulfilling 1 < e < f (n) and moderately prime to f (n) i.e., gcd (e, f (z)) = 1.
4. Figure a number d with the end goal that d = e-1 mod f (n).
5. Encryption: Enter message to get figure content. Ciphertext c= mod ((message. ^e), N).
6. Decoding: The figure content is unscrambled by: Message=mod ((c. ^d), N) [14]

.

2.6. *Steganography:*

Steganography is disguised composition and is the logical methodology of embeddings the mystery information inside a spread media with the end goal that the unapproved watchers don't get a thought of any data covered up in it. Steganography is an option in contrast to cryptography where the emit information is inserted into the transporter so that lone bearer is unmistakable which is sent from transmitter to beneficiary without scrambling. Steganography is the craft of concealing the presence of information in another transmission medium to accomplish mystery correspondence. It doesn't supplant cryptography yet it very well may be utilized to improve the security of cryptography [15].

The secret data can be embedded into the spread media by the stego framework encoder with utilizing certain calculation. A mystery message can be plaintext, a picture, ciphertext , or anything which can be spoken to in type of a bitstream. After the mystery date is installed in the spread article, the spread item will be called as a stego object additionally the stego article sends to the beneficiary by choosing the reasonable channel, where decoder framework is utilized with the equivalent stego strategy for getting unique data as the sender might want to move. There are different sorts of steganography [15]. Figure 2 shows the steganography system.

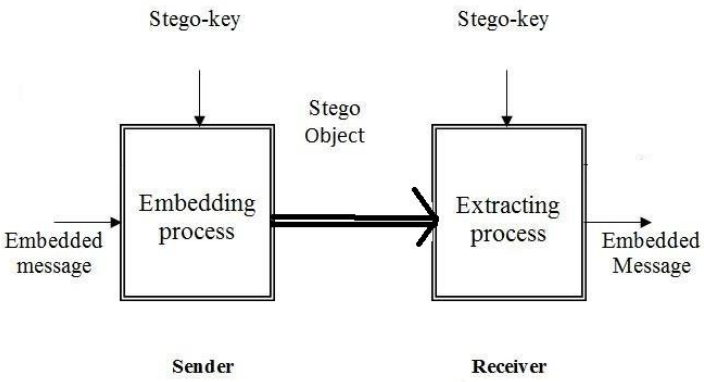

Fig. 2

Steganography can be part into two kinds:
a) Fragile: This steganography includes installing data into a record which is devastated if the document is changed.
b) Robust: Robust checking expects to install data into a record which can only with significant effort be obliterated.

2.6.1. *LSB Technique:*

In Least Significant Bit (LSB) steganography insert the instant message in least noteworthy bits of computerized picture. In which information is installed by supplanting the LSB of spread bearer with the information to be send.ie first perused the spread picture and instant message which is to be covered up in the spread picture, at that point convert instant message in double. Ascertain LSB of every pixel of spread picture. Supplant LSB of spread picture with each piece of mystery message individually so we get a picture wherein information is covered up [16].

For instance, the accompanying network can be considered as 3 pixels of a 24-piece shading picture, utilizing 9 bytes of memory

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

For this situation, just three bits should have been changed to embed the character effectively. By and

large, just 50% of the bits in a picture should be altered to conceal a mystery message utilizing the maximal spread size. The outcome changes that are made to the least huge bits are too little to be in any way perceived by the human visual framework (HVS), so the message is successfully covered up.

III. CONCLUSIONS

Cryptography and steganography are outstanding techniques for information security. To upgrade the security we can utilize consolidated cryptography and steganography as opposed to utilizing cryptography or steganography alone. In this paper we have checked on different mixes of cryptography and steganography techniques. Breaking a steganographic framework needs the aggressor to distinguish that steganography has been utilized and he can peruse the installed message. As indicated by, steganography gives methods for mystery correspondence, which can't be evacuated without fundamentally modifying the information where it is inserted. What's more, the security of old style steganography framework depends on mystery of the information encoding framework. When the encoding framework is known, the steganography framework is vanquished.

REFERENCES

[1] F. A. P. Petitcolas et al, "Information Hiding-A Survey," Proceedings of the IEEE, special issue on protection of multimedia content, Vol. 87, Issue. 7 PP. 1062-1078, July 1999.

[2] Seth, D., Ramanathan, L., Pandey, A. "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010, pp. 3-6.

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

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

[5] Das,R., Das, I. "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques", IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016.

[6] Indrayani,R., AdiNugroho,H., Hidayat,R., Pratama,I. "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function", International Conference on Science and Technology-Computer (ICST), IEEE, 2016.

[7] Johnson, N.F. and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, IEEE, Vol. 31, pp. 26-34, 1998.

[8] Singh,A. "An Improved LSB based Image Steganography Technique for RGB Images", Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015, pp 1-4.

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

[10] Karthikeyan, B., Kosaraju, A. C. and Gupta, S. "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.

[11] Dhamija, A. and Dhaka, V. "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.

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

[13] Sharma, H., Sharma, K. K. and Chauhan, S. "Steganography techniques using cryptography-a review paper," 2014.

[14] kumar, A., Sharma,R. "*A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[15] Hussain,M and Hussain,M. "A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[16] Dr. Walia ,E., Jain ,P., Navdeep . "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology Vol. 10 Issue 1 (Ver 1.0), April 2010.

[17] Varsha, Dr. Singh,R. C. " Data Hiding Using Steganography and Cryptography", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April-2015, pg. 802-805.