Secret Message Hiding Technique For Raw Intelligence Service Using Image Processing

Kulkarni Dinesh G.[1], MasuteSumit C[2], Vanmoresachin T.[3], Kamblevijaykumar B.[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[1, 2, 3, 4] Brahmdevdada Mane Institute Of Technology, Solapur

Abstract- *Securing the information becomes all the more necessary. In the current situation, raw security is very much needed. For example, if I want to send to India what is being planned against India, then I can send it in encryption format. Because of this, no one else will understand that information. Because of this, no one will be able to attack our country easily. This will give impetus to the progress of our country. It is also involved in the security of India's nuclear program Many foreign analysts consider the RAW to be an effective organization and identify it as one of the primary instruments of India's national power. Gathering foreign intelligence, advising Indian policymakers on counterterrorism, and advancing India's foreign strategic interests counter-proliferation, is the agency's primary function.*

Keywords- RAW Security, Steganography, image security, data hiding.

I. INTRODUCTION

In today's world, communication is important as well as necessary technology in the modern world. Its basic goal is sharing and transferring data but this technology is not safe at a certain level. Steganography was derived from the Greek word stegano, meaning covered or secret, and graphic (writing or drawing) [1]. the rapid development of technologies leads to increase interest in the field of hiding information in images, audio, etc. "Embedding" is the process of concealing the data inside any multimedia types like audio, video, etc. The main reason to use steganography is that valuable information is transferred from one place to another insecurely and unreliably. Heraeus communicate with his son-in-law in Greece. the message onto the slave's scalp shaved the head of one of his slaves and tattooed. the slave has dispatched with the hidden message when the slave's hair grew back [2]. Steganography leads to making it difficult to tell either a secret message exists at all or not. If an unauthorized third party is able to say with high confidence that a file contains a secret message, then steganography has failed [3]. This paper intends to give an overview of image steganography and its uses and hiding the files (text file, an audio file, etc) by using LSB and AES algorithm.

THE NEED FOR RAWSECURITY

Steganography.it is hiding one piece of data to hiding information into digital multimedia files and also at the network packet level, steganography is the solution. n adjoining countries, it can monitor the political and military developments, It direct bearing on India's national security and in the formulation of its foreign policy.Steganography. it is hiding one piece of data to hiding information into digital multimedia files and also at the network packet level, steganography is the solution. n adjoining countries, it can monitor the political and military developments, It direct bearing on India's national security and in the formulation of its foreign policy.

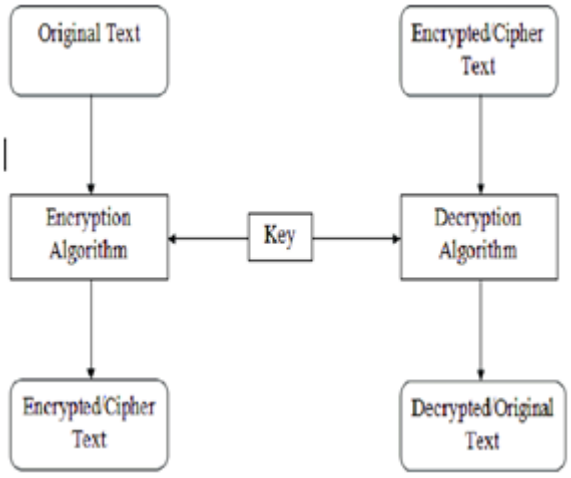


Fig: Block Diagram

II. PROCESS OF ENCRYPTING IMAGE

Data owner:

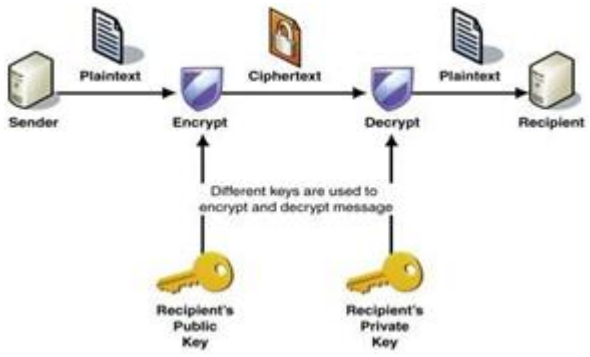
To upload it into the external data storing center for ease of sharing or for cost-saving the client who owns data and wishes. (attribute-based) access policy and enforcing it on its own data by encrypting the data under the policy before distributing it.a data owner is responsible for defining.

User:

It is an entity that wants to access the data. the access policy of the encrypted data and is not revoked in any of the valid attribute groups user possesses a set of attributes satisfying, to decrypt the ciphertext and obtain the data then he will be able. Since both of the key managers, the KGC and the data storing center, are semi-trusted, they should be deterred from accessing the plaintext of the data to be shared; meanwhile, to issue secret keys to users they should be still able. In order to realize this somewhat contradictory requirement, the two parties engage in the arithmetic 2PCprotocol with master secret keys of their own, and issue independent key components to users during the key issuing phase. none of them can generate the whole set of secret keys of users individually 2PC protocol deters them from knowing each other's master secrets.

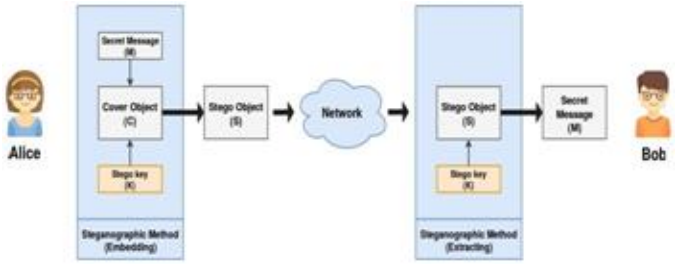
III. OVERALL SCENARIO

In Secrete communication, Steganography is the smart way of invisible communication. hiding the existence of the communicated information is nothing but hiding information in other information, thus. In image, steganography is nothing but, information that can be overlaps or hidden exclusively in image properties. Extremely difficult to detect, a normal cove message was sent over an insecure channel with one of the periods on the paper containing hidden information. it is carriers and networks the high-speed delivery channels.& mostly used on computers with digital data.



IV. METHODOLOGY

In the proposed scheme the main target is to develop a secure technique for messages transformations so that secret information can be successfully sent over the various network in a protected and secure manner without countered into any kind of attacks by an unintended user image files is The most popular medium because of their high easy availability & most used over the internet . the sender's, end the image used for embedding the secret information image is called cover image, and the secret information that needs to be protected is called a secret transferred message. As soon as data can be embedded by applying various appropriate embedding algorithm, then it is called stego image processing



This Encrypted image is transferred to the receiver over the network, and he extracts out the same secret message using various appropriate extraction algorithm And there is Another data hiding technique, called cryptography is also used for the secure transmission of messages over the internet, but most popular technic is steganography & it is becoming most used because of its various advantages over cryptography. Cryptography can only hide the exact meaning of a message from the third-party user or notaries user whereas steganography successfully hides the large existence of the message itself. Figure shows the Steganography System.

V. CONCLUSION

In wider ways Steganography is not implemented and used but it is the best security tool. The main problem of today's world is to secure and maintain their data confidentially, the techniques used currently which can only be replaced by Steganography. are not considered the best .

Inviable communication is very present in whole internet virtual communication today.In digital media there are two important uses of data hiding one of them is to provide proof of the copyright and assurance of content integrity in data security.

On another hand in various applications of data hiding, such as the type of inclusion augmentation data, is not necessary to be invariant to detection, for the benefit of both the author and the content consumer.

REFERENCES

[1] Sneha, B. and Gunjan, B (2014) Data Encryption by Image Steganography. International Journal of Information and Computation Technology, 4, 453-458. http:// www.irphouse.c om/ijict.htm

[2] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001
[3] Philip Bateman and Dr. Hans “Image Steganography and Steganalysis”, M.S., Department of Computing Faculty of Engineering and Physical Sciences, University of Surrey Guildford Surrey,United Kingdom, 2008.
[4] Hiding data in images by simple LSB substitution by ChiKwong Chan, L.M.Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.
[5] S. Dickman, An Overview of Steganography, Research Report JMU- INFOSEC-TR -2007-002, James Madison University, July, 2007.
[6] S.B.Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.
[7] ”A Tutorial Review on Steganography” by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and PoulamiDas,Heritage Institute of Technology.
[8] An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science Universityof Pretoria, 0002, Pretoria, South Africa.
[9] Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on , vol., no., pp.1188,1193, 20-21 March 2013.
[10] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385