e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 5, May 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

| DOI:10.15680/IJMRSET.2024.0705060 |

An Approach for Secure Data Encryption and Decryption Using Crypto-Stego

Vishakha Subhash Raut, Dr. Anand Singh Rajawat

M. Tech (CTIS) Student, Dept. of Computer Science and Engineering, Sandip University, Mahiravani, Nashik, Maharashtra, India

Assistant Professor, Dept. of Computer Science and Engineering, Sandip University, Mahiravani, Nashik, Maharashtra, India

ABSTRACT: Due to recent developments in stego analysis, providing security of personal content, messages, or digital images using steganography has become increasingly difficult. By using stego analysis, one can easily disclose the presence of hidden information in company car files. The project introduces a new steganographic method of communication between two independent groups. The approach presented in this project uses both steganographic and cryptographic techniques. In Cryptography we use RSA. At Steganography we use Image Steganography to hide data. We also use the Integrated Verification process to satisfy all Cryptography resources namely, Access Control, Confidentiality, Integrity, Verification. This way we can store data more securely. As we use the RSA algorithm to protect data and again this time, we do Steganography to hide the data in the image. So that anyone else in the network can access existing data on the network. Only the sender and recipient can retrieve the message from the data.

KEYWORDS: Rivest-Shamir-Adleman (RSA), Cryptography, Steganography.

I. INTRODUCTION

Digital communication witnesses a noticeable and continuous development in many applications on the Internet. Therefore, secure communication sessions should be provided. The security of data distributed across the global network has become an important factor in network performance measurement. Therefore, confidentiality and integrity of data are required to prevent the audience from accessing and using the transmitted data. Steganography and Cryptography are two important methods used to provide network security. The aim of this project is to develop a new way to encrypt confidential information, using the benefits of combining cryptography with steganography. Cryptography is one of the traditional methods used to ensure the confidentiality of communication between the parties. This method is a secret writing technique, used to encrypt a plain text into a ciphertext that will be transmitted between the sides in an unprotected channel. By using a valid key, the ciphertext can be encrypted into a real clear text. Without key information, no one can retrieve plain text. Cryptography plays an important role in many aspects of secure communication, such as confidentiality, confidentiality, non-denial, key exchanges, and authentication. Cryptography is one of the methods used to ensure confidential communication between parties. This method is a secret writing technique, used to encrypt a blank text into a ciphertext that will be transmitted between the sides in an unprotected channel. By using a valid key, the ciphertext can be encrypted into a real clear text. Without key information, no one can retrieve plain text. Cryptography plays a key role in many of the things needed to secure a secure connection to a secure channel, such as confidentiality, privacy, non-refusal, important exchanges, and authentication. It can be defined as the science of encryption and data communications by trusted network companies in an attempt to hide the existence of data. Therefore, there is no information on the original message. If one looks at the cover where the information is hidden inside, one will not have the knowledge that there is cover data, this way one will not try to decrypt the data. Confidential information can be entered into the stego system encoder using a specific algorithm. A private message can be plain text, an image, a ciphertext text, and anything else that can be represented in the form of bitstream. After the confidential data is embedded in the cover, the cover object will be called the stego object and the stego object will be sent to the recipient by selecting the appropriate channel, where the decoder system is used in the same way to get the original information as the sender would like to transfer.

II. RELATED WORK

Cryptography has followed man through many stages of evolution. Cryptography can be traced back to 1900 B.C. to an ancient Egyptian writer who used unconventional texts in inscriptions. From 500 - 600 B.C. The Hebrew writers used ATBASH, a retractable alphabet for a simple solution. From 50 - 60 B.C. Julius Caesar used a simple word instead of the usual verbs in government communication. Cryptography continued history with the May variety. Today cryptography has reached a new level, quantum cryptography. Quantum cryptography combines physics and cryptography to produce a new invincible cryptosystem without the sender and receiver having experience of tried and failed interventions. With a long history of cryptography, steganography was developed and prospered on its own. Steganography comes from the Greek steganos (covered or secret) and -graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages among others, seemingly harmless messages, graphics or sounds. The first steganographic method was invented in ancient Greece about 440 BC Greek Emperor Histaeus used the first version of steganography which included: shaving a slave's head, writing a message on a slave's skin, waiting for a hair growth to reveal a secret message, and sending a slave on a journey. The recipient will have a slave head to reveal the message. The recipient can respond in the same way to steganography. At the same time, another early steganography method was used. This method involved Demerstu, who wrote a letter to the Spartans warning of an impending attack from Xerxes. The message was engraved on a wax tablet, then covered with a new layer of glue. This seemingly empty tablet was successfully delivered with its hidden message. Steganography continued to evolve in the early 1600s as Sir Francis Bacon used the variation of the facial expression to treat each part of the code text. Small dots were complete text, photographs, and layouts reduced to period size and attached to standard paper. Null ciphers are also used to convey private messages. Null ciphers are unencrypted messages with real messages embedded in the current text. Hidden messages were hard to translate inside innocent messages. An example of an innocent message containing a null cipher is: Fishing for freshwater curves and salty shore rewards anyone who feels depressed. Experienced angler anglers often find smart escapees entertaining and admit that the quality of the swordfish is beyond their capacity at any time. By taking the third letter in each word the following message appears: Send Attorneys, Guns, and Money.

III. PROPOSED WORK

In this section, we will discuss the proposed method that combines two different encryption methods, namely Cryptography and Steganography. In the first proposed method, the message is encrypted using the RSA algorithm. Next, we use a modified LSB method to embed the encrypted information into an image. Thus, this process combines features of both cryptography and steganography and provides a high level of security. It is better than any other method used separately. There will be an agreement between the sender and the receiver regarding the encryption algorithm key and the encryption algorithm key or these keys can be exchanged via secure communication. Our method starts by encrypting first and then encrypting encrypted data. Before using cryptography and steganography, we first convert our input to Base-64. We also store the resulting text in a text file. Then we move on to cryptography and steganography.

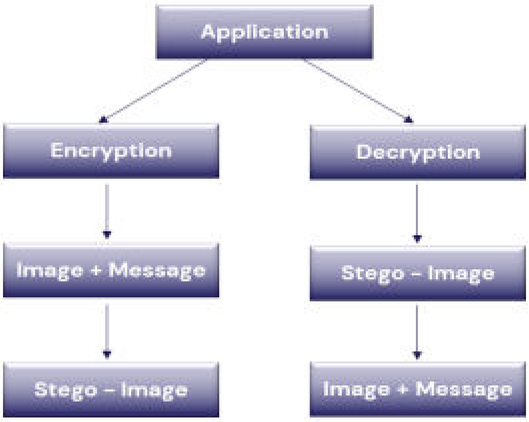

Fig. 1 System Architecture

Encryption The senders' category contains cryptographic and steganography categories. This method starts with cryptographic and then steganography. In the cryptographic phase, we use the RSA algorithm (Rivest Shamir Adelson). This process takes two prime numbers. Encryption can be done using plain text and "e" values generated using two prime numbers. After that we will receive the cipher text, which is passed to the end of the receiver for decryption. This encrypted data will be used in the steganography phase.

In the stenography phase, we use the LSB algorithm (Least Significant Bit) with some modification to hide information (encrypted data from the encryption phase) inside the cover. We use the image as a cover to introduce our method, but this method can also be used for other files such as audio, and video. The most common LSB method is used to hide confidential information in a file; the last part of each pixel or sample or frame used consecutively to hide one of the bits of binary streaming cover Encryption cover image.

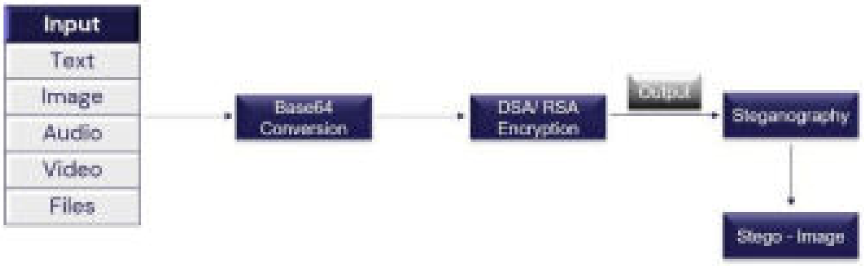

Fig. 2 Encryption Mechanism Overview

Receiver side consists of steganography and cryptography stages. On the receiver side we will first extract embedded data then decrypt it. On the receiver side, we start with steganography and then cryptography. We will use the same steps which are used on the sender side. In the cryptography stage, we use the data which is extracted from the stego file and use RSA. We will use the same steps which are used on the sender side. The Decryption can be done using the Encrypted message, receiver's private key and sender's public key. Plain Text is now in Base-64 mode. After receiving the plain text, use Base-64 conversion to convert the blank text into a given input, which can be Text, Image, Video, Audio.

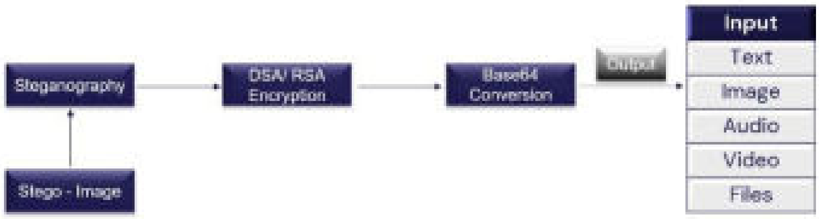

Fig. 3. Decryption Mechanism Overview

To get a picture of steganography we use Spatial techniques. Geographically, the most widely used is the LSB substitution method. Least important bit (LSB) method is a simple, easy way to embed information in a cover file. In steganography, the LSB method is used instead. i.e., as each image has three parts (RGB). This pixel information is stored in a single-coded format. The first bits contain this information in all pixels that can be changed to keep the text hidden. In this case, the first condition is that the text to be saved must be smaller or equal to the size of the image used to encrypt the text. The LSB based method is a local domain method. But this is at risk of cracking and noise. In this way, the MSB (most important pieces) of the message to be hidden are stored in the LSB (at least the key pieces) of the image used as the cover image. The Human Visual System (HVS) cannot detect changes in color or pixel intensity when the LSB bit is adjusted. This is a repetition of the mind and the visual as this can be used as an advantage to store information in these pieces but still not notice the major differences in the image.

IV. RESULTS AND ANALYSIS

It is noteworthy that steganography and cryptography alone are not sufficient for information security, so if we combine these systems, we can produce a more reliable and robust approach. The combination of these two strategies will improve information security. This combination will meet the requirements, for example, memory location, security, and the ability to transfer important information to an open channel. Also, it will be a powerful way for people to communicate without the distraction of the audience without even knowing that there is a way to communicate in the first place.

V. CONCLUSION

We are dealing with security ideas for digital data communications across the network. This project is designed to integrate steganography with encryption features for better performance. We developed a new method of steganography and integrated it with the RSA algorithm. The data is hidden in the image so there will be no chance of the attacker knowing that the data is hidden in the image. We made our way into the picture by using a program written in Python language. The proposed method has been shown to be effective in hiding different types of text, images, sound and videos in colored images. We concluded that in our way the Image and RSA files were better. Because of their high volume. This function introduces a system that can transmit large amounts of confidential information and provide secure communication between two private organizations. Both steganography and cryptography can be woven into this system to make finding very difficult. Any type of text data can be used as a private message. A secret message using the concept of steganography is sent over the network. In addition, the proposed process is simple and easy to use. Data embedding is done such as audio, video, and photo embedding, by selecting a different and new image, which can prevent the attacker from accessing hidden data. The results obtained indicate that our proposed approach is encouraging in terms of safety, and durability.

REFERENCES

[1] M. E. Saleh, A. A. Aly, and F. A. Omara, “Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding,” International Journal of Computer Science and Security (IJCSS), Volume (9), Issue (2), pp. 397 - 397, 2015

[2] 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.

[3] K. R. Babu et al, “A Survey on Cryptography and Steganography Methods for Information Security,” International Journal of Computer Applications (0975 – 8887), Vol. 12, No.2, PP. 13-17, November 2010

[4] R. Oppliger, “SSL and TLS: Theory and Practice,” ARTECH HOUSE, 2014.

[5] B. Schneier, “Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth),” pp. 1–1027, January 1996.

[6] H.Abdulzahra, R. AHMAD, and N. M. NOOR, “Security enhancement; Combining cryptography and steganography for data hiding in images,” ACACOS, Applied Computational Science,pp.978-960,2014.

[7] P. R. Ekatpure and R. N.Benkar, “A comparative study of steganography & cryptography,”2013.

[8] M. H. Rajyaguru, “Cryptography-combination of cryptography and steganography with rapidly changing keys,” International Journal of Emerging Technology and Advanced Engineering, ISSN, pp.2250-2459,2012.

[9] D. Seth. L. Ramanathan, and A.Pandey, “Security enhancement; Combining cryptography and steganography,” International Journal of Computer Applications (0975-8887) Volume,2010.

[10] J. V. Karthik and B. V. Reddy, “Authentication of secret information in image steganography,” International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6. P. 58. 2014.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com