IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306133|

An Approach for Secure Data Encryptionand Decryption Using Crypto-Stego

Vishakha Raut, Dr. Anand Singh Rajwat, Dr. Mohammad Muqeem, Dr. Pawan R. Bhaladhare.

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

Professor, Department of Computer Science and Engineering, Sandip University, 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 senderand recipient can retrieve the message from the data.

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

I. INTRODUCTION

Digital communication witnesses a clear and continuous development in many applications within the Internet. Hence, secure communication sessions must be provided. The security of data that is transmitted across a world wide network has become a key factor on the network performance measures. So, the confidentiality and integrity of transmitted data are needed to stop from accessing and using transmitted data. Steganography and Cryptography are 2 techniques that are provided for network security. The aim of this paper is to develop an approachto cover secret data in an image, by takingadvantage of combination of cryptography and steganography.

Cryptography is one of the secure method used to guarantee the privacy of communication between parties. This method is used for secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext are often decrypted to the given plaintext. Cryptography provides a secure communication across an insecure channel, like: confidentiality, privacy, non-repudiation, key exchange, and authentication. There are two kinds of Cryptography techniques : i) Symmetric / Secret Key Cryptography ii) Asymmetric / Public Key Cryptography.

Cryptography is one of the methods used to ensure confidentialcommunication between parties. This method is a secret writingtechnique, used to encrypt a blank text into a ciphertext that will be transmitted between the sides in an unprotected channel. Byusing 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, suchas 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 onthe 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 thedata. 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 elsethat can be represented in the form of bitstream. After the confidential data is embedded in the cover, the cover object willbe called the stego object and the stego object will be sent to therecipient 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.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306133|

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 treateach 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 thecurrent 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 convertour input to Base-64. We also store the resulting text in a text file. Then we move on to cryptography and steganography.

FIGURE AND TABLE

Algorithm
Inputs: Image, Message, Key.
1) Initially Senders consider a Cover Image.
2) Hide the Encrypted message in the image.
3) Hiding can be done using a secret key for confidentiality.
4) After Hiding the Image is considered as a Stego-Image.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306133|

Which consists
of image and data which is encrypted.

5) The Receiver will receive the Stego-Image.
6) Using the Secret Key, the receiver can view the data hiddenin the image.
7) Thus, the receiver can receive the message safely.

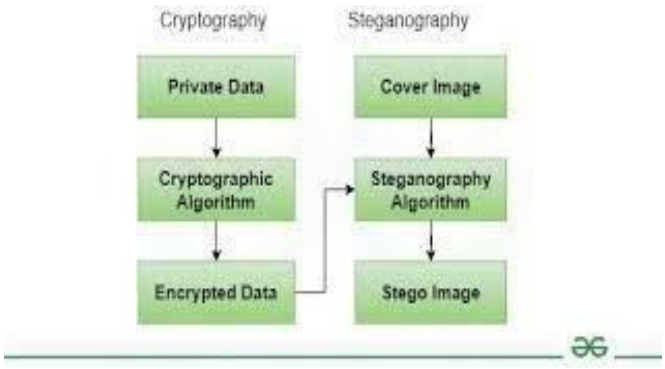

Fig. 1 System Architecture

Encryption

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

Encryption is a mathematical process that alters data using an encryption algorithm and a key. Imagine if Alice sends the message "Hello" to Bob, but she replaces each letter in her message with the letter that comes two places later in the alphabet. Instead of "Hello," her message now reads "Jgnnq." Fortunately, Bob knows that the key is "2" and can decrypt hermessage back to "Hello."

Alice used an extremely simple encryption algorithm to encode her message to Bob. More complicated encryption algorithms canfurther scramble the message

Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext. Truly secure encryption will use keys complex enough that a third party is highly unlikely to decrypt or break the ciphertext by brute force — in other words,by guessing the key. (Alice's first encryption method would be broken very quickly.)

Data can be encrypted "at rest," when it is stored, or "in transit,"while it is being transmitted somewhere else.

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.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306133|

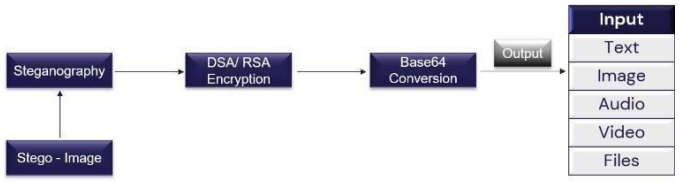

Fig. 2. Decryption Mechanism Overview

LSB Positioning Method

This method is an easy way to hide data within a given image. We use LSB bits pixels within the given image. When converting an image to a digital format, we often choose between three different color representations:

- 24-bit color: Each pixel can have one of 2 ^ 24 colors, and this is represented by different values of three basic colors: red (R), green (G), blue (b) given 8 bits
- (256) each.
- 8-bit color: Each pixel can have one color in 256(2 ^ 28), selected palette, or color table.
- 8-bit gray scale: Each pixel can have one in 256 shades(2 ^ 28) of gray.

LSB installation converts LSBs for each color in 24-bit images, or LSBs for 8-bit value in 8-bit images. The most basic of LSBinserts in 24-bit images include 3 bits / pixel.

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 tothe 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.

WHY BASE 64?

Base64 is also widely used for sending e-mail attachments, because SMTP – in its original form – was designed to transport7-bit ASCII characters only. Encoding an attachment as Base64 before sending, and then decoding when received, assures older SMTP servers will not interfere with the attachment.

IV. RESULT AND ANALYSIS

It is noteworthy that steganography and cryptography alone arenot 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

In this project, we deal with the concepts of security of digital data communication across the network. This project is designed by using the steganography and cryptography features factors for better performance. We performed a new steganography method and combined it with RSA Encrption algorithm. We performed our method on image by

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306133|

implementing a program written in Python language. The method proposed has proved successful in hiding various types of text, images, audio and videos in colour images. We concluded that in our method the Image files and RSA Cryptography are better . Because of their high capacity. Results achieved indicate that our proposed method is encouraging in terms of security and robustnesscommunication between two private organizations. Both steganography and cryptography can be woven into this systemto make finding very difficult. Any type of text data can be usedas 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 photoembedding, 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 interms 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. 7PP. 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 cryptograhy 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,” Interntional 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 ofComputer Applications (0975-8887)Volume,2010.
10. J. V. Karthik and B. V. Reddy, “Authentication of secret information inimage steganography,” International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6. P. 58. 2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details