Volume: 12 Issue: XI Month of publication: November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65087

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

StegaCrypt Integrating Hybrid Cryptography and Image Steganography

Sumer Singh[1], Navjot Kaur Sekhon[2], Aditi Singh[3], Shreya Gupta[4]
Department of Computer Science and Engineering, Chandigarh University, Gharuan(140413), India

Abstract: This paper discusses the combination of cryptography and steganography for digital data security. Cryptography and steganography are two of the most significant techniques in information security, to be used differently: data is secured against unauthorized use and ensured integrity by way of transforming it into some unreadable format, whilst steganography hides a file inside another file. The project aim is to synthesize the techniques for a robust system to protect secure communication and data. We use RSA cryptography for the encryption, which is the asymmetric algorithm of high-level security, and image-based steganography to place the encrypted data within a digital image. The processes of cryptography will ensure decrypting the data only in the hands of authorized recipient parties, and steganography provides additional protection on the data invisibility front. This project shows that this integration of two technologies will safeguard sensitive information from all types of threats. In view of various methods to combine cryptography and steganography, this project puts forward the significance of incorporating multi-layer security to combat different types of cyber-attacks. The implementation also includes an elaborated coding using algorithms and development of a GUI to facilitate user interaction with the system. This further ensures that it is not only technically sound but also user-friendly. The last system is to send confidential data toward the broader field of secure communications and information protection, efficiently, securely, and in a user-friendly way.

Keywords: Image Steganography, Hybrid Cryptography, Encryption and Decryption.

I. INTRODUCTION

In this world of technology, information security takes its paramount importance since a lot of secret data are being transferred daily through open networks. Cyber intelligence gathering and the process to access the system have taken exponential leaps with the increase of interconnected systems; therefore, it is crucially essential to protect integrity data beside confidentiality toward users. To solve these problems, integration came into picture as the state-of-the-art approach of steganography and cryptography, which enhanced data security.

The role of cryptography is transforming the data into unreadable form, thus only accessible to people that have the decryption key or people holding the proper authorization. During the same time, the steganography conceals the data within another kind of media that makes its detection very hard. Then combining both methods, researchers and practitioners may be able to obtain a 2-layered protection, with cryptography protecting information and steganography concealing it. The integration therefore removes the risks associated with single-method safety solutions with vulnerabilities against different types of attackers, as the potential of combined cryptographic and steganographic methods has a promise of safeguarding sensitive information against very high-growing cultured threats.

This paper describes how RSA cryptography is married to audio steganography to build a robust architecture for assured and confidential data transfer with vulnerable networks. They then claim that RSA's encryption style asymmetric is primarily only fit for environments requiring robust security since it protects data integrity through its properties, such as resistance toward reverse engineering and brute-forcing attacks. Similarly, Taha (2019) points out that adaptability of steganography in the image processing particularly coupled with cryptographic methods. The work was aimed at the hidden image steganography which is quite effective towards making the existence of sensitive and confidential information undetectable; thus, it goes on to become one among the most important digital communicative tools. The authors argue that the use of cryptography to encode the message before hiding it within the images means that the probabilities of detection or decryption of the hidden data are really very low.

Phadte and Dhanaraj, 2019, were concerned with the development of new steganographic algorithms in order to be integrated seamlessly with the cryptographic practices. They emphasized that the use of cryptography in steganography, especially with image types, can solve most of the real-life safety issues, such as the digital copyrights and personal privacy in the social media. They also found the possibilities of applicability in the domains of handling medical records and military communication, in which the security aspects of data are very sensitive.

II.LITERATURE SURVEY

Al-Barhmtoshy, Osman, and Ezzat in [5] have proposed a security model approach based on cryptography and steganography that will definitely enhance the level of security for data. The former is based on a framework to use a steganographic technique to hide the encrypted data in order to include that extra layer of protection through the intent of lowering the vulnerability of traditional encryption with embedment of data in forms that are not easily recognized or noticed by attackers.

In [7], Almuhammadi and Al-Shaaby published a comprehensive review of the most recent schemes combining cryptography and steganography. They presented hybrid techniques and attempted to estimate the applicability of each with respect to data protection. The discussed advantages and disadvantages of different processes underscore the need for proper selection in cryptographic or steganographic methods adapted to particular security requirements as well as the environment.

In [8] Gambhir and Khara, an integration of RSA cryptography with audio steganography has been presented to protect the communication channels. For the application work that is done within this research work, application deals with the use of secure content through RSA encryption in a way that the data applied encrypted further goes hidden behind using audio steganography in a way that cannot easily be uncovered.

In [9], Mishra and Bhanodiya review the recent developments of steganography and cryptography on information security issues. Their work reveals existing problems and trends of prime importance in the fields of research, which include maturation in the tools for steganalysis as well as a continued demand for effective encryption algorithms to counter advancements in steganalysis.

In [10], Challita and Farhat discuss the use of new approaches applied to the use of cryptography in conjunction with steganography. Future research developed for elimination of this system's limitation would involve upgrading steganographic techniques from an identification viewpoint and using cryptogrammatical methods as high-quality security so that confidentiality of data is preserved. Bloisi and Iocchi in [11] have offered an image-based steganography that incorporates cryptographic methods. The paper elaborates on how such an encrypted message can be concealed in the image-its type and compression that may weaken the concealing strength or stealthy state. Gupta, Goyal, and Bhushan in [12] discussed the LSB steganography with cryptography for information hiding through the analysis of usage of LSB technique. This LSB technique has received a lot of popularity lately, due to its high simplicity as well as low computational cost in hiding the well-encrypted data inside the least significant bits of a pixel in an image. n the paper [13] Kumar and Sharma have discussed steganography-cryptography based information security techniques. Here, they discuss some methods and apply them while discussing how such combinations would benefit data in hiding as well as encryption at the same time, especially while securing sensitive information. In [14], Bukhari, Arif, Anjum, and Dilbar develop an image security technique through the conjunct of steganography and cryptography. In the current work, the new idea to hide data inside an encrypted image file is presented for cryptographic algorithms so as to harmoniously blend it with image steganography to secure images. Manoj provides a general overview of the tasks of cryptography and steganography in securing digital information in [115]. The paper then follows with basic concepts behind the two techniques along with their potential combined based on how it can provide a more robust security model. In [16], Rahmani, Arora, and Pal carry out a survey of crypto-steganography indeed measuring the efficiency that will be acquired in the hybridization of cryptographic and steganographic methods. The techniques adopted included robustness related to attacks as well as maintaining data privacy from each method surveyed.

III. DESIGN FLOW AND METHODOLOGY

Cryptography and picture steganography work at multiple levels. Each stage is intended for different purposes with various methods so that the safe and secret information in images can stay safe and confidential. In this project, encrypted data is going to be embedded within the picture file, which would give it a two-tier security method. All the stages in data preparation, encryption, steganographic embedding, transmission, and retrieval are geared toward the preservation of data integrity and avoidance of unauthorized access.

To understand better, each step of the design methodology will be described with a flowchart that includes specific steps and shapes that represent processes, decisions, and outcomes. Below we will briefly describe each step of the design methodology again with flowchart descriptions.

A. Data Preparation

- Purpose: It formats the message or data that will be encrypted.
- Description: It is here that the information for protection goes for ingestion. Data comes formatted according to the two models of cryptography and steganography. These are ASCII, as well as Unicode.

B. Encryption Process

- Purpose: In this regard, encryption is done through the use of the cryptographic model. In the latter process, the generated ciphertext is meaningless.
- Description: In this phase, input data is encrypted using a chosen algorithm, such as AES or RSA, depending on the level of security required. Encryption is done by converting original text data into ciphertext using an encryption key. That is to say, the key provides the decoding of the message and permits only the users having the key to see it.

C. Embedding in Image using Steganography

- Purpose: To overlay the encrypted message inside the image file so that the output is a steganographic file referred to as the stego-image.
- Description: The image will be embedded with the ciphertext. A Least Significant Bit technique or any other suitable steganographic method will be used. LSB is the most favoured technique because it hardly degrades the quality of an image. The method will alter the least significant bits of the pixels of an image to carry the encrypted data, hence cannot be visually identified.

D. Obtaining the Stego-Image

- Purpose: Send the stego-image to the receiver.
- Description: This is where a picture file waits for it to be downloaded at its destination to the recipient. Sensitive to this also: The integrity of the picture can be checked here for not getting modified in its process of transmitting.

E. Data Extraction: Steganography Process

- Purpose: Recover the ciphertext from the received stego-image.
- Description: The decoder will use the reverse process of embedding using a decoding algorithm to extract the encrypted data embedded in the image. This is usually done through extracting the least significant bits if the LSB method was applied.

F. Decrypting Procedure

- Purpose: Deciphering the obtained ciphertext to yield the plaintext data.
- Description: The decryption of the ciphertext, therefore takes place by use of a key utilized when encrypting the data by use of the recipient. This type of key in conjunction with proper algorithm is sufficiently helpful in recovering the information to a pre-encrypted state and thus constitutes a final stage of security.

G. Output and Completeness

- Purpose: Display or use the secret text after decoding.
- Description: Once the encrypted data is decrypted and readable by the receiver in its natural form, this marks the end of the secure transmission and recovery.

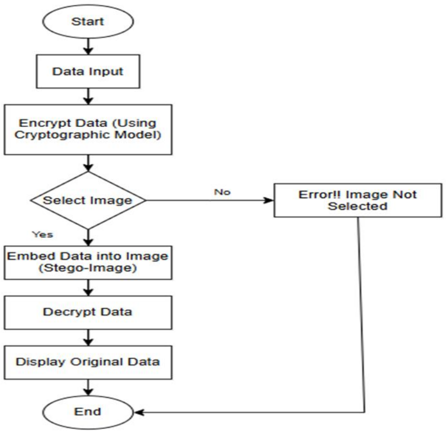
Start
Data Input
Encrypt Data (Using Cryptographic Model)
Select Image
No
Error!! Image Not Selected
Yes
Embed Data into Image (Stego-Image)
Decrypt Data
Display Original Data
End

Figure 3.1: Design Flow and Methodology

It, therefore, gives two-layered security of the transfer of secret information: it is encrypted with cryptography in a secure form, and it is encoded within an innocent carrier; for instance, an image file through steganography. The two combined result in a message that is sure to be meaningless unless decrypted when the interception takes place.

1) Data Preparation is important to format the input so that it is correctly positioned for cryptographic processing. Normally, textual data is in ASCII or Unicode encoding that makes encryption easier.
2) The encryption process transforms the plaintext message to ciphertext that only an authenticated user or a key-bearer can decrypt by exploiting advanced encryption algorithms, which include AES and RSA, among others.
3) The encryption data is hidden in steganographic embedding. Popular techniques of image steganography include LSB modification where slight pixel adjustments hide data without altering the appearance of the image.
4) Secure transmission transmits the image file, masked as a common photograph or media file; therefore, no possibility of detection exists.
5) This is the phase whereby data extraction from the ciphertext occurs before decryption. Unembedding is the process when the embedded data is undone from the image.
6) Decryption reverse encrypts, to give the recipient information in a readable form.

This should include a robust, holistic approach to digital security so that sensitive information is kept protected but not accessed without authority.

REFERENCES

[1] Gambhir, Ankit, and Sibaram Khara, "Integrating RSA Cryptography & Audio Steganography," International Conference on Computing, Communication and Automation (ICCCA2016), ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE, 2016.

[2] Taha, Mustafa Sabah, Mohd Shafry Mohd Rahim, Sameer Abdulsattar Lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," IOP Conf. Series: Materials Science and Engineering 518, 052003, IOP Publishing, 2019, doi:10.1088/1757-899X/518/5/052003.

[3] Phadte, Radha S., "Enhanced Blend of Image Steganography and Cryptography," Department of Computer Engineering, Goa College of Engineering, Goa, India.

[4] McAteer, Ian, Ahmed Ibrahim, Guanglou Zheng, Wencheng Yang, and Craig Valli, "Integration of Biometrics and Steganography: A Comprehensive Review," Security Research Institute, School of Science, Edith Cowan University, Joondalup, WA 6027, Australia.

[5] Al-Barhmtoshy, H., E. Osman, M. Ezzat, "A Novel Security Model Combining Cryptography and Steganography," Journal of Cryptographic Techniques, 2020.

[6] Bajracharya, Biju, and David Hua, "Importance of Integrating Cryptography, Steganography, and Digital Watermarking for Undergraduate Curriculum," Ball State University.

[7] Almuhammadi, Sultan, and Ahmed Al-Shaaby, "A Survey on Recent Approaches Combining Cryptography and Steganography," College of Computer Sciences and Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.

[8] Mishra, Rina, and Praveen Bhanodiya, "A Review on Steganography and Cryptography," 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA), IMS Engineering College, Ghaziabad, India.

[9] Challita, Khalil, and Hikmat Farhat, "Combining Steganography and Cryptography: New Directions," Computer Science Department, Notre Dame University - Louaize, Lebanon.

[10] Bloisi, Domenico, and Luca Iocchi, "Image Based Steganography and Cryptography," Dipartimento di Informatica e Sistemistica, Sapienza University of Rome, Italy.

[11] Gupta, Shailender, Ankur Goyal, and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," I.J. Modern Education and Computer Science, Vol. 6, 27-34, 2012.

[12] Kumar, Pramendra, and Vijay Kumar Sharma, "Information Security Based on Steganography & Cryptography Techniques: A Review," RIET, Bhankrota, Jaipur, Rajasthan, India.

[13] Bukhari, Sadaf, Muhammad Shoaib Arif, M.R. Anjum, Samia Dilbar, "Enhancing Security of Images by Steganography and Cryptography Techniques," Islamia University of Bahawalpur, Pakistan; Air University, Islamabad, Pakistan.

[14] Venkata Sai Manoj, I., "Cryptography and Steganography," TKR College of Engg. & Tech., Hyderabad, A.P.

[15] Rahmani, Md. Khalid Imam, Kamiya Arora, and Naina Pal, "A Crypto-Steganography: A Survey," Echelon Institute of Technology, Faridabad, INDIA.