IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 5, May 2024

The Art of Digital Disguise: Image Cryptography and Steganography

Santosh Chauhan[1], Sejal Gunjal[2], Pratiksha Jadhav[3], Dr. Mahesh Maurya[4]

Students, Department of Computer Engineering[1,2,3]
Head of the Department, Department of Computer Engineering[4]
K. C. College of Engineering, Thane, India

Abstract: *Securing data through encryption and decryption is vital in today's digital landscape. However, recent advancements in steganalysis have posed challenges to the security of personal content, messages, and digital images concealed using steganography. The emergence of stego analysis techniques has made it easier to detect hidden information within carrier files. To address these challenges, this project proposes a novel approach that combines steganographic and cryptographic methods for secure communication between two private parties. In the realm of cryptography, the RSA algorithm is employed for encryption and decryption. Meanwhile, image steganography is utilized to conceal the encrypted data within images. Additionally, a mutual authentication process is integrated to fulfill the essential services of cryptography, including access control, confidentiality, integrity, and authentication. This comprehensive approach ensures robust security measures for data transmission and storage. By leveraging RSA encryption followed by image steganography, unauthorized access to the data present in the network is thwarted. Only the intended sender and receiver possess the means to retrieve the message from the concealed data, ensuring confidentiality and privacy.*

Keywords: Rivest-Shamií-Adleman(RSA), Cíyptogíaphy, Steganogíaphy

I. INTRODUCTION

In the constantly changing environment of digital communication, ensuring secure transmission of data has become crucial. As more and more apps pop up online, having strong communication is super important. The security of data navigating global networks has emerged as a critical aspect influencing network performance metrics. Ensuring that data remains confidential and intact is crucial to prevent unauthorized access by eavesdroppers. To tackle these worries, two important methods, steganography and cryptography, are key to making networks more secure. Steganography hides secret messages in innocent-looking files, while cryptography ensures the encryption and decryption of data to keep it safe and intact. The main goal of this project is to create a new way of hiding secret messages in images by combining cryptography and steganography. We want to use the strengths of both methods to make digital communication safer and stronger, and to reduce the risks from possible attackers.

Cryptography

Cryptography is an age-old technique employed to ensure the confidentiality of communication between individuals or groups. It involves encoding the original message with a secret key, turning it into a scrambled version known as ciphertext. The encoded message can only be decoded back to its oíiginal foím by someone who possesses the appíopíiate key. Without this key, accessing the original message is impossible. Cryptography serves crucial functions in enabling secure communication over insecure channels, including maintaining confidentiality, privacy, nonrepudiation, facilitating key exchange, and verifying the authenticity of messages

Symmetric / Secret Key Cryptography

Symmetric or secret key cryptography, also referred to as symmetric-key, shared-key, single-key, or private- key encryption, involves using a single key for both encrypting and decrypting data. This key is kept confidentialand is known only to authorized individuals for encryption and decryption purposes. When a sender encrypts plaintext using this key, the same key is used by the receiver to decrypt the message and retrieve the original plaintext. While this technique

DOI: 10.48175/568

provides robust security for data transmission, the challenge lies in securely distributing the key. If the key is stolen or compromised, it can lead to unauthorized access to the encrypted datawithout difficulty. An example of symmetric-key cryptography is the DES Algorithm.

Asymmetric / Public key cryptography

Asymmetric or public key cryptography, also known as asymmetric cryptosystem, utilizes a pair of mathematically related keys, one for encryption and the other for decryption. Unlike symmetric cryptography, where the same key is used for both operations, in asymmetric cryptography, the encryption and decryption keys are separate. When data is encrypted with the public key, it can only be decrypted using the corresponding private key, ensuring that the data remains secure. The public key, used for encryption, is openly available, while the private key, used for decryption, is kept confidential. An example of an asymmetric-key algorithm isRSA.

Steganography

Steganography can be defined as the practice of concealing and transmitting data within seemingly innocuous carriers, aiming to keep the existence of the data hidden. When someone views the carrier containing the hiddeninformation, they are unaware of its presence, preventing them from attempting to decipher it. The steganographic encoder uses specific algorithms to embed secret information into the carrier medium. This secret data can take various forms, such as plaintext, images, or ciphertext, represented as a stream of bits. Oncethe secret data is embedded, the carrier becomes known as a steganographic object, which is then sent to the receiver through a suitable channel. The receiver uses a decoder system employing the same steganographic method to extract the original information as intended by the sender.

Advantage of Steganography and Cryptography

It is evident that solely employing either steganography or cryptography may not be adequate to ensure comprehensive information security. Thus, by integrating these two systems, we can develop a more thoroughand robust approach. The combination of steganography and cryptography enhances the security of informationtransmission by addressing various requirements such as memory space, overall security, and the strength of encryption.

II. LITERATURE SURVEY

SR. NO.	YEAR	AUTHORS	TITLE	FINDINGS
1	2020	Ridhima Ahluwalia, Dr. Anish Gupta, Dr. Priyanka Chaudhary	Steganography: Double Encrypted Image Deployed in Cloud	Data Compression, Encryption & Steganography Techniques to Enhance Data Security & Transmission Efficiency. Similar Approach, Along With Cloud Deployment
2	2021	Osama Fouad Abdel Wahab, Ashraf A. M.Khalaf, Aziza I. Hussein, Hesham F. A. Hamed	Hiding Data Using Efficient Combination Of Rsa Cryptography, And Compression Steganography Techniques	Data Compression, Encryption & Steganography Techniques to Enhance Data Security & Transmission Efficiency. Used Techniques Such As Lossy & Lossless CompressionAlong With Rsa.
3	2020	Dalia Mubarak Alsaffar, Atheer Sultan Almutiri, Bashaier Al Qahtani	Image Encryption Based On Aes And Rsa Algorithm	The results showed that the aes algorithm correlation coefficient tends to be closer to the zero, thus astronger correlation.
4	2021	K. Pavani,	Enhancing Public Key	This Approach Increases The Security Of

		P. Sri Ramya	Cryptography Using RSA, RSA-CRT And N- Prime RSA With Multiple Keys	The RSA Algorithm By Using Four Public Key Pairs. It Could Mainly Be Focused On Running Attacks That Can Be Viable On Rsa, Thus Providing Multiple Key Cryptosystems For Specifically Rsa And Enhancing Full Performance
5	2020	Matcha Venkatesh, T. Anitha, G. Satish, M.Sudarshan, K.Ram Sudeep	Secure Data Encryption and Decryption Using Crypto-Stego	This Paper Proposes A Novel Approach Combining RSA Cryptography, Image Steganography, and Mutual Authentication To Enhance Data Security And Convert Communication

III. PROPOSED METHOD

Analysis

The implementation of this method is meticulously executed through the development of a Python based program, meticulously crafted to cater to the intricacies of image processing. Through this program, the proposed method is systematically applied to manipulate images, effectively embedding diverse types of data, encompassing text, images within the pixel data of color images. This comprehensive approach ensures that the concealed data remains imperceptible to unauthorized viewers, thus fortifying the confidentiality of transmittedinformation.

Problem Definition

The purpose of this project is to provide the correct data with security to the users.The encoded message can only be decoded back to its original form by someone who possesses the appropriate key. Our application will give youmore Security to the data present in the network and there will be able to reduce the loss of data in the networkwhich will be transmitted from the sender to the receiver using the latest technologies. Only the Authorized persons i.e., who are using our application will be there in the Network.

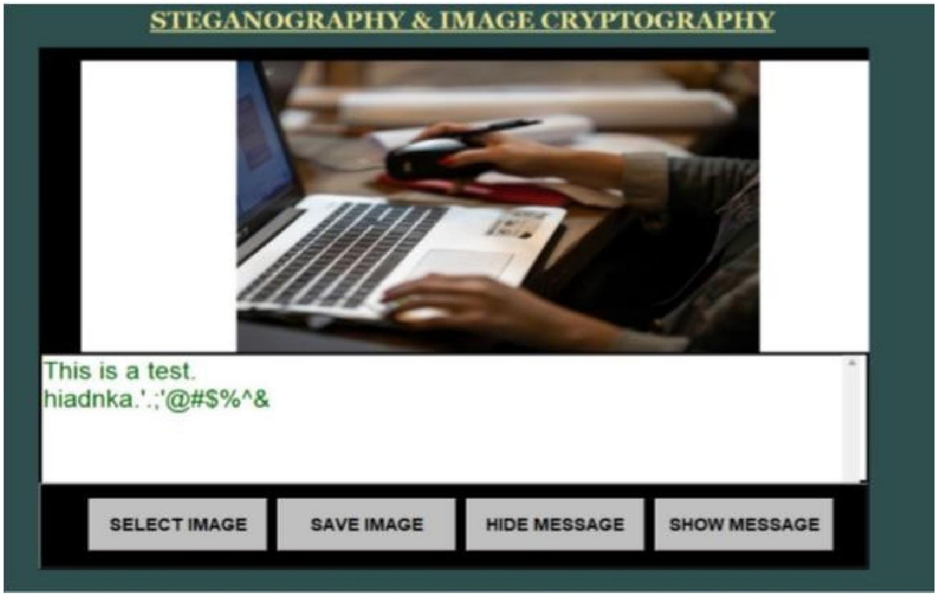
Feasibility Study

A feasibility study is a crucial element of a project report, assessing the practicality and likelihood of success of a proposed endeavor in data encryption and decryption. It examines technical, financial, economic, and social factors to gauge the project's viability and whether it warrants pursuit. Through comprehensive analysis, a feasibility study furnishes essential insights to aid stakeholders in making informed decisions, mitigating risks, optimizing resource allocation, and enhancing the prospects of project accomplishment

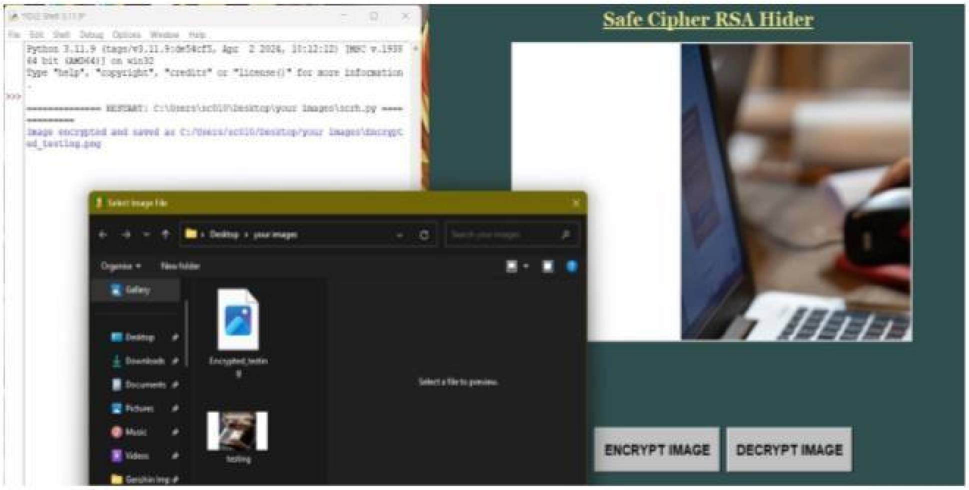
IV. IMPLEMENTATION

The algorithm is to hide the text data effectively in an image without any suspicion of the data being hidden in the image.To defend against attacks, utilizing a unique and novel image that defies comparison without resorting to plagiarism is essential.. The aim of the project is to hide the data in an image using steganographyand ensure that the quality of concealing data must not be lost. We used a method for hiding the data in a distinct image file in order to securely send over the network without any suspicion of the data being hidden. This algorithm, though, requires a distinct image which we can use as a carrier and hide the data which is well within the limits of the threshold that employing an image capable of concealing data can provide robust security measures.

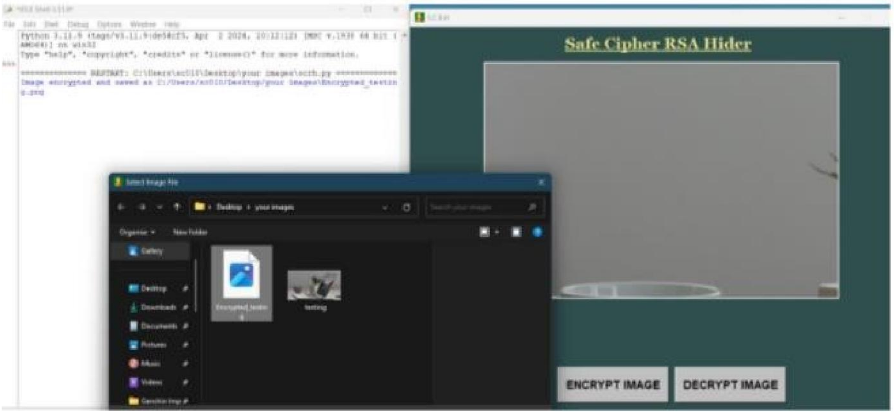
PART A - Hiding message in cover image and then encrypting the image.



This is a test.
hiadnka.'.;'@#$%^&



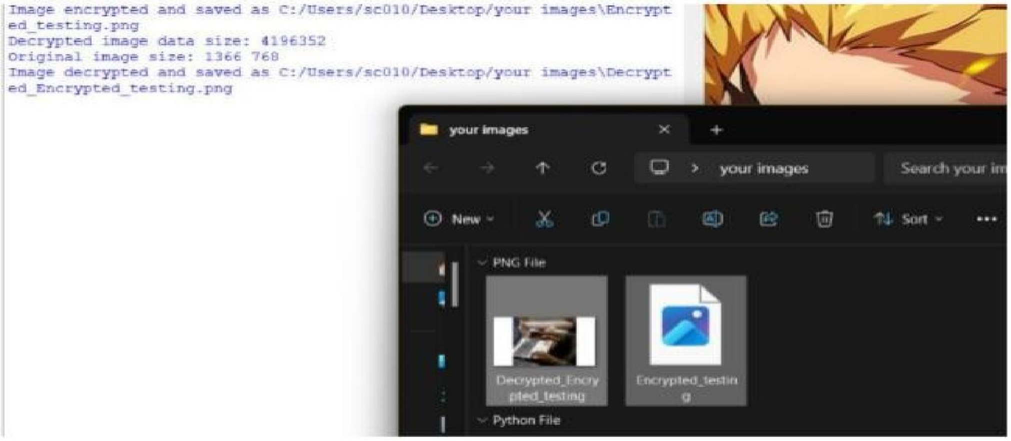
```
Python 3.11.9 (tags/v3.11.9:de54cf5, Apr  2 2024, 10:12:12) [MSC v.1938
64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information
.
>>>
=============== RESTART: C:\Users\sc010\Desktop\your images\scrh.py ====
=========
Image encrypted and saved as C:/Users/sc010/Desktop/your images\Encrypt
ed_testing.png
```



```
Python 3.11.9 (tags/v3.11.9:de54cf5, Apr  2 2024, 10:12:12) [MSC v.1938 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
=============== RESTART: C:\Users\sc010\Desktop\your images\scrh.py ==============
Image encrypted and saved as C:/Users/sc010/Desktop/your images\Encrypted_testin
g.png
```

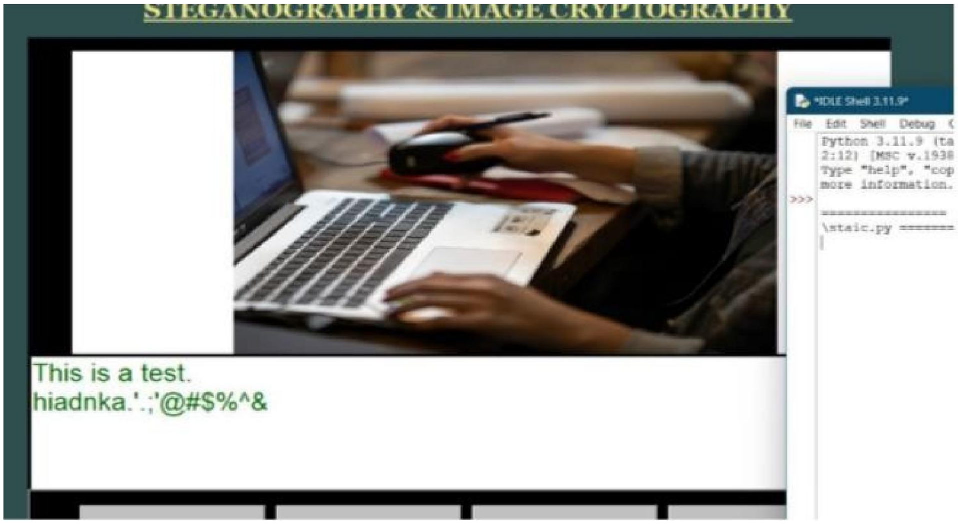
DOI: 10.48175/568

PART B - Image decryption and extraction of hidden message from image.



```
Image encrypted and saved as C:/Users/sc010/Desktop/your images\Encrypt
ed_testing.png
Decrypted image data size: 4196352
Original image size: 1366 768
Image decrypted and saved as C:/Users/sc010/Desktop/your images\Decrypt
ed_Encrypted_testing.png
```

PART C - Successful extraction of message after Stegano+RSA Application.



This is a test.
hiadnka.'.;'@#$%^&

```
Python 3.11.9 (ta
2:12) [MSC v.1938
Type "help", "cop
more information.
>>>
=================
\staic.py =======
```

V. FUTURE SCOPE & CONCLUSION

This project focuses on enhancing the security of digital data communication over networks by integrating steganography and cryptography. A novel steganography technique was developed and combined with the RSA algorithm for data encryption and decryption. By concealing data within images, the method prevents attackers from detecting the hidden information. Implementation was carried out using Python programming language.

The proposed approach has been successful in hiding various forms of data, including text, images. The utilization of image files and RSA encryption was found to be advantageous due to their high data capacity. The project introduces a system capable of transmitting large volumes of secret information securely between two parties.

Both steganography and cryptography are intertwined in this system to heighten detection complexity. Any form of text data can serve as a secret message. The steganographically encoded secret message is then transmitted over the network. Moreover, the proposed procedure is straightforward and easy to implement.

Although RSA is a reliable, strong and secure algorithm, the only drawback it faces is the 'Key Sharing', since RSA is an asymmetric method it uses different keys for both encryption and decryption. Using a symmetric algorithm such as AES will eliminate the key sharing problem as it uses the same key for both encryption and decryption.

DOI: 10.48175/568

REFERENCES

[1]. Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques.

[2]. Steganography: Double Encrypted Image Deployed In Cloud. [3]. Secure data encryption and decryption using crypto-stego. [4]. Image steganography: A review of the Recent Advances.

[5]. Image encryption based on AES and RSA algorithms.

[6]. Enhancing public key cryptography using RSA,RSA-CRT and N-Prime RSA with multiple keys