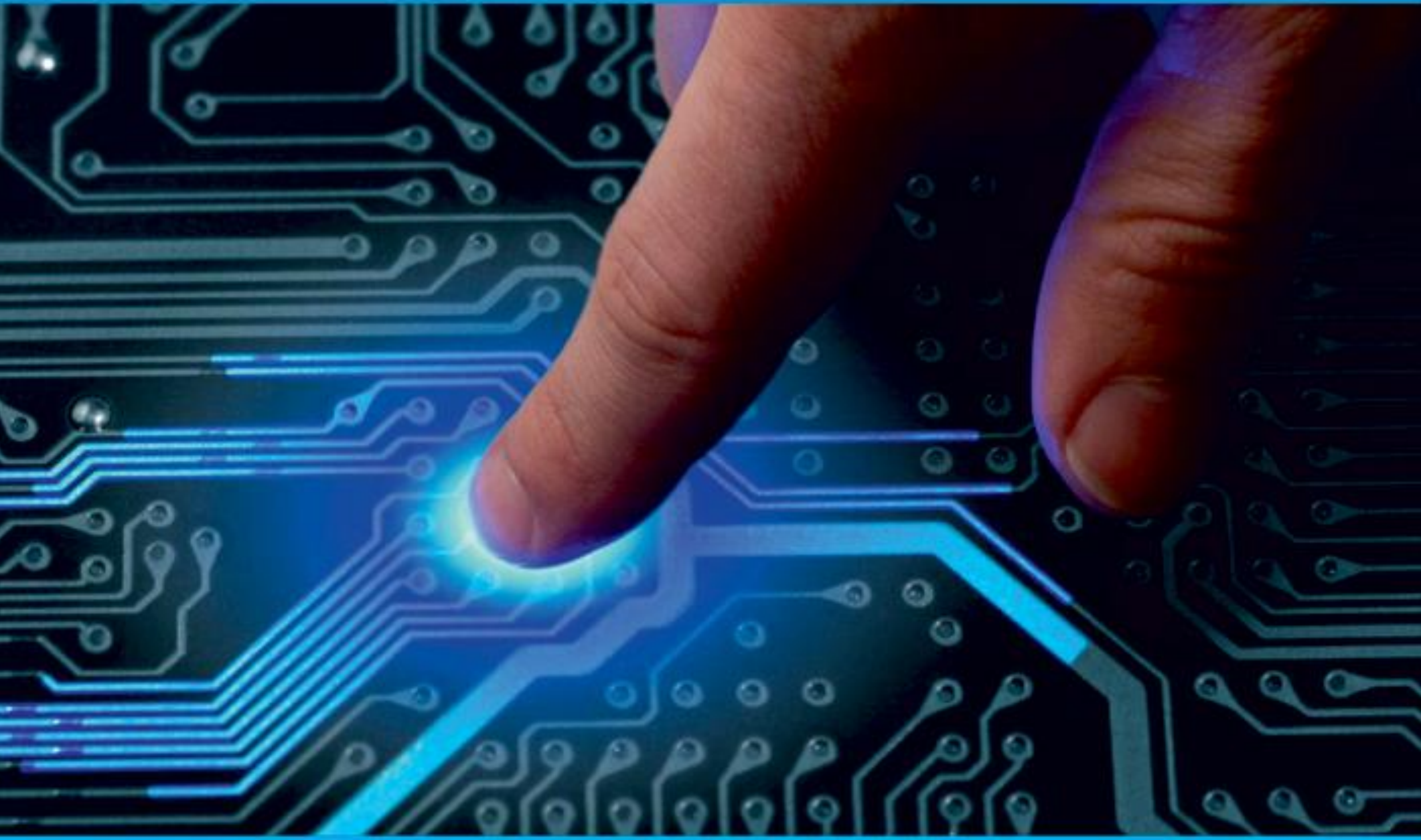
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204221 |

Secure Transmission of Confidential Crime Document Using Steganography Techniques

Dr.M.Priya, B.Baranidharan, M.Maajid, B.Devibalan

Associate Professor, Department of Computer Science, Engineering, E.G.S. Pillay Engineering College, Nagapattinam, India

U.G. Student, Department of Computer Science Engineering, E.G.S. Pillay Engineering College,Nagapattinam, India

U.G. Student, Department of Computer Science Engineering, E.G.S. Pillay Engineering College,Nagapattinam, India

U.G. Student, Department of Computer Science Engineering, E.G.S. Pillay Engineering College,Nagapattinam, India

ABSTRACT: In today's digital age, ensuring the confidentiality and security of sensitive information, particularly in the realm of law enforcement and crime investigation, is paramount. Traditional methods of data transmission are often vulnerable to interception and unauthorized access. To address this challenge, this paper proposes a novel approach leveraging image steganography for the secure transmission of confidential crime documents.

Steganography is the art of concealing information within seemingly innocuous cover media. By embedding sensitive textual data within digital images, we can obfuscate the existence of the concealed information, making it difficult for adversaries to detect. The proposed method involves encoding textual crime documents into the least significant bits (LSBs) of selected pixels in an image, exploiting the imperceptible alterations to the cover image.

To ensure robustness and security, cryptographic techniques such as encryption and authentication are integrated into the steganographic process. Prior to embedding, the plaintext crime documents are encrypted using a strong encryption algorithm, rendering them unintelligible without the corresponding decryption key. Additionally, digital signatures or message authentication codes (MACs) are employed to verify the authenticity and integrity of the transmitted document

I. INTRODUCTION

In the realm of law enforcement and crime investigation, ensuring the confidentiality and security of sensitive information during transmission is crucial. Conventional methods of data transmission often lack robustness against interception and unauthorized access. To address this challenge, the proposed approach leverages image steganography techniques for secure transmission of confidential crime documents.

Steganography is the art of concealing information within seemingly innocuous cover media. By embedding textual crime documents into digital images, the existence of concealed information is obfuscated, making it difficult for adversaries to detect. This technique involves encoding the plaintext documents into the least significant bits (LSBs) of selected pixels in the image.To enhance security, cryptographic techniques such as encryption and authentication are integrated into the steganographic process. Before embedding, the crime documents are encrypted using a strong encryption algorithm, rendering them unintelligible without the decryption key. Digital signatures or message authentication codes (MACs) are employed to verify the authenticity and integrity of the transmitted documents, further enhancing security.

Advanced steganographic algorithms such as adaptive LSB substitution or spatial domain techniques are utilized to improve stealthiness and resistance against detection. These methods dynamically adjust the embedding strategy based on image characteristics, minimizing the statistical detectability of the hidden information.

II. WORKING PRINCIPLE

Steganography is the practice of concealing a message, image, or file within another message, image, or file in a way that the existence of the hidden content is not readily apparent. Here's a general working principle for securely transmitting a confidential crime document using steganography techniques:

Document Selection: Choose the confidential crime document that needs to be transmitted securely. This document should contain sensitive information that needs to be protected from unauthorized access.

Steganography Technique Selection: Select a steganography technique that suits your requirements. There are various steganography techniques available, including hiding data within images, audio files, video files, or even text documents. Choose a technique that provides a suitable balance between security and feasibility for your specific scenario.

Embedding Process: Embed the confidential crime document within a carrier file using the chosen steganography technique. This typically involves modifying certain bits or properties of the carrier file to encode the hidden document. The embedding process should be carefully performed to ensure that the carrier file appears unchanged to casual observers.

Transmission: Once the confidential document has been embedded within the carrier file, transmit the carrier file through a secure channel to the intended recipient. Ensure that the transmission channel itself is secure to prevent interception or tampering by unauthorized parties.

Reception: The recipient of the carrier file must be aware of the steganography technique used and possess the necessary decryption or extraction tools to recover the embedded confidential document. They should use these tools to extract the hidden document from the carrier file.

Decryption/Extraction: Decrypt or extract the embedded confidential document from the carrier file using the appropriate steganography tools and techniques. This process should be performed securely to prevent unauthorized access to the sensitive information.

Verification: Verify the integrity and authenticity of the extracted confidential document to ensure that it has not been altered or tampered with during transmission. Compare it with the original document to confirm its accuracy.

Secure Storage: Safely store the extracted confidential document in a secure location to prevent unauthorized access. Implement appropriate security measures, such as encryption and access controls, to protect the document from unauthorized disclosure.

By following these steps, you can securely transmit a confidential crime document using steganography techniques, ensuring that the sensitive information remains protected from unauthorized access or interception.

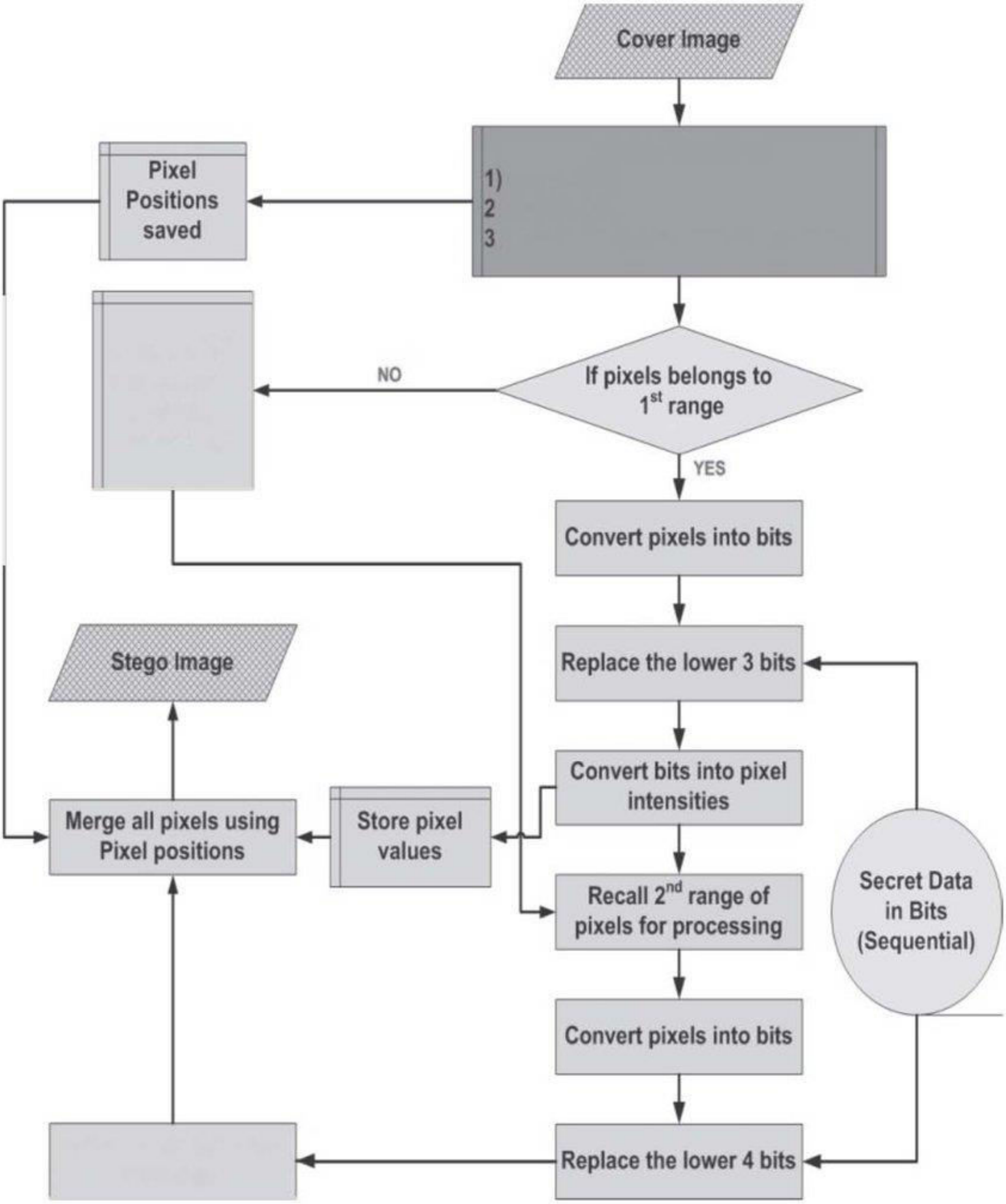
III. ARCHITECTURE DIAGRAM

The diagram you sent depicts a system for securely transmitting a confidential crime document using steganography techniques. Steganography is a technique for hiding information within a seemingly harmless cover file, such as an image, audio file, or video. In the context of the diagram, the confidential crime document is hidden inside a cover file to make it undetectable during transmission.

The process begins with the client, which could be a law enforcement officer or investigator, requesting to transmit a confidential crime document. Upon receiving the transmission request, the server acknowledges the request and initiates the encryption process. It's important to note that the diagram doesn't show the specific encryption method used. The confidential crime document, presumably after encryption, is then embedded into a cover file using steganography. There are various steganography techniques, some of which modify the least significant bit (LSB) of the cover file to embed the message data.The document, now hidden inside the cover file, is transmitted from the client to the server.The server receives the disguised file and extracts the hidden confidential crime document. It's likely that the server decrypts the document using the same method used to encrypt it earlier.Finally, the server retrieves the original confidential crime document and sends it to its destination, which may be another authorized user on the network.
Steganography offers an extra layer of security by making the confidential information undetectable during transmission.Steganography is not a foolproof method and there are techniques to detect the presence of hidden messages.

Overall, the system depicted in the diagram offers a two-pronged approach to securing the transmission of confidential crime documents. Steganography helps mask the existence of the confidential data, while encryption protects the confidentiality of the information itself.The effectiveness of steganography depends on the chosen technique. Techniques that embed large amounts of data may distort the cover file enough to be noticeable. Using robust techniques and balancing data size with imperceptibility are important considerations.

Overall, the system depicted in the offers a two-pronged approach to securing the transmission of confidential crime documents. Steganography helps mask the existence of the confidential data, while encryption (if used) protects the identialityoftheinformationitself.


Cover Image
1)
2
3
Pixel Positions saved
NO
If pixels belongs to 1st range
YES
Convert pixels into bits
Replace the lower 3 bits
Stego Image
Convert bits into pixel intensities
Merge all pixels using Pixel positions
Store pixel values
Recall 2nd range of pixels for processing
Secret Data in Bits (Sequential)
Convert pixels into bits
Replace the lower 4 bits

IV. METHODOLOGY

Methodology for securely transmitting a confidential crime document using steganography techniques:

Document Selection and Encryption:
Select the confidential crime document that needs to be transmitted securely.
Encrypt the document using a strong encryption algorithm and a secure key. This step ensures that even if the carrier file is intercepted, the confidential information remains protected.

Steganography Technique Selection:
Choose a steganography technique suitable for your requirements and the type of carrier file you'll use (e.g., image, audio, video).
Consider factors such as the capacity of the carrier file, robustness against various attacks, and compatibility with transmission channels.

Embedding Process:
Select a suitable carrier file (e.g., an image, audio file) that will conceal the encrypted crime document.
Embed the encrypted document into the carrier file using the chosen steganography technique.
Ensure that the embedding process does not visibly alter the carrier file, maintaining its appearance and characteristics to avoid suspicion.

Transmission Preparation:
Prepare a secure channel for transmitting the carrier file. This could involve using encrypted communication protocols, secure file transfer methods, or physical delivery in secure storage media.

Transmission:
Transmit the carrier file containing the embedded encrypted crime document through the secure channel to the intended recipient.
Take precautions to prevent interception or tampering during transmission, such as using encrypted connections, secure file transfer protocols, or physical couriers for delivery.

Reception:
The recipient receives the carrier file and prepares to extract the embedded encrypted document.
Ensure that the recipient has access to the necessary steganography tools and decryption keys required to extract and decrypt the confidential information.

Extraction and Decryption:
Use steganography tools to extract the encrypted crime document from the carrier file.
Decrypt the extracted document using the appropriate decryption key to recover the original confidential content.

Verification and Authentication:
Verify the integrity and authenticity of the decrypted crime document to ensure it has not been altered or tampered with during transmission.
Compare the decrypted document with the original encrypted document to confirm its accuracy and completeness.

Secure Storage and Handling:
Safely store the decrypted crime document in a secure location, applying additional security measures such as encryption, access controls, and backups.
Implement secure handling procedures to prevent unauthorized access, disclosure, or loss of the confidential information**.**

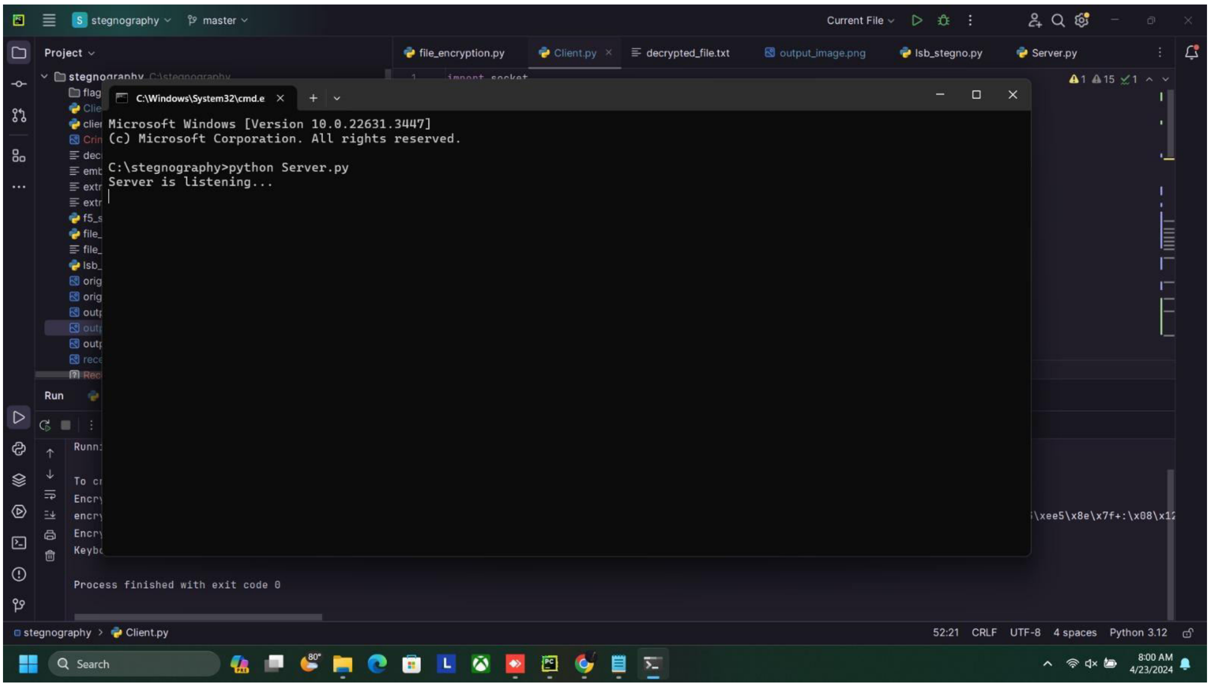
Documentation and Audit:
Maintain detailed records of the transmission process, including the steganography techniques used, encryption keys, transmission channels, and recipient information.

Conduct regular audits and reviews to ensure compliance with security policies and identify any vulnerabilities or weaknesses in the transmission process.

By following this methodology, you can securely transmit a confidential crime document using steganography techniques, safeguarding the sensitive information from unauthorized access or interception.

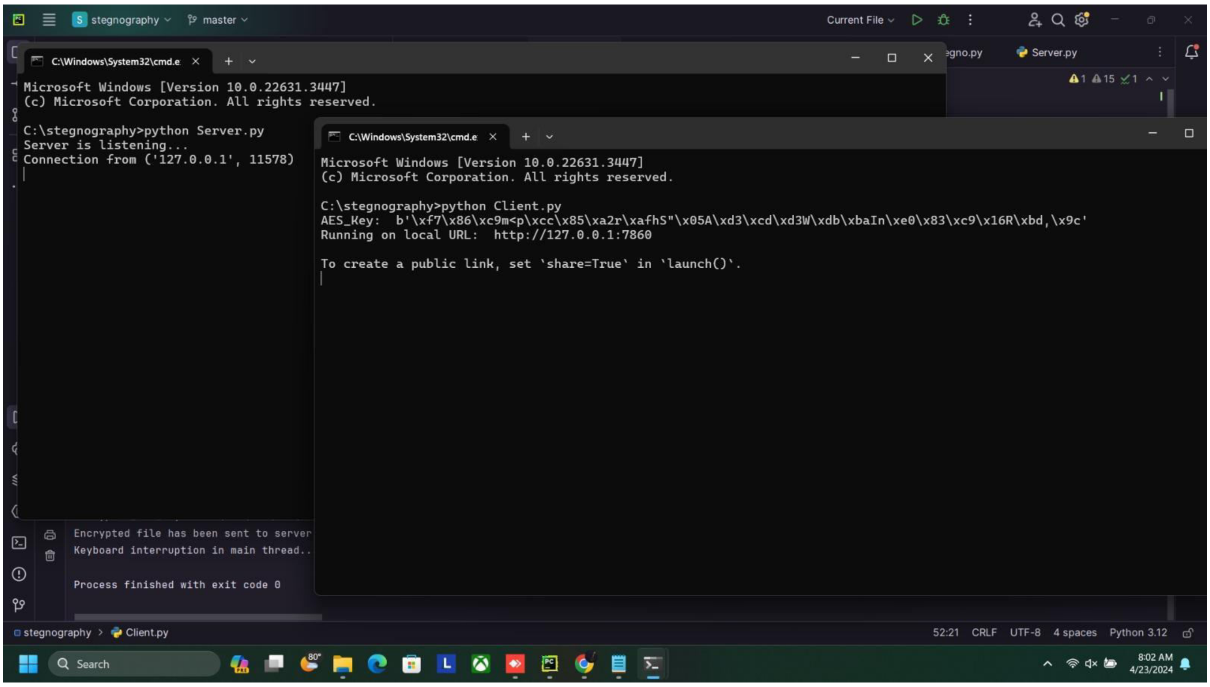
V. EXPERIMENTAL RESULT

1. STARTING SERVER



```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\stegnography>python Server.py
Server is listening...
```

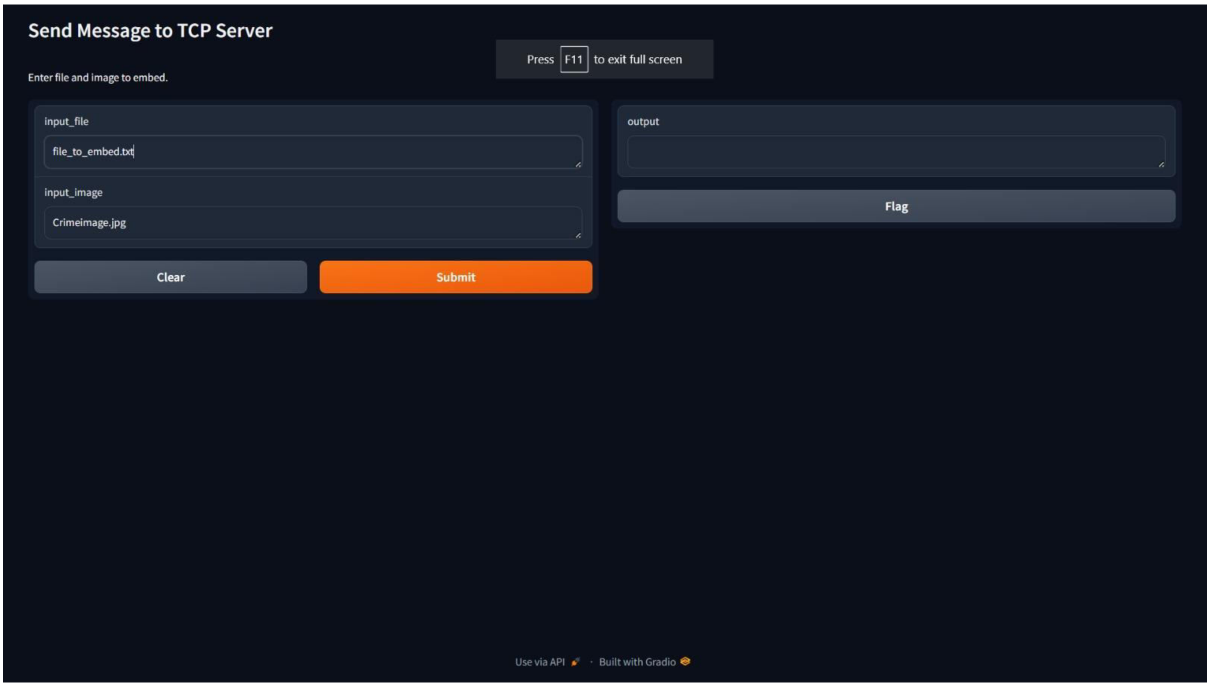
2. STARTING THE CLIENT



```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\stegnography>python Server.py
Server is listening...
Connection from ('127.0.0.1', 11578)
```

```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\stegnography>python Client.py
AES_Key:  b'\xf7\x86\xc9m<p\xcc\x85\xa2r\xafhS"\x05A\xd3\xcd\xd3W\xdb\xbaIn\xe0\x83\xc9\x16R\xbd,\x9c'
Running on local URL:  http://127.0.0.1:7860

To create a public link, set `share=True` in `launch()`.
```

3 .CLIENT UI


Send Message to TCP Server

Enter file and image to embed.

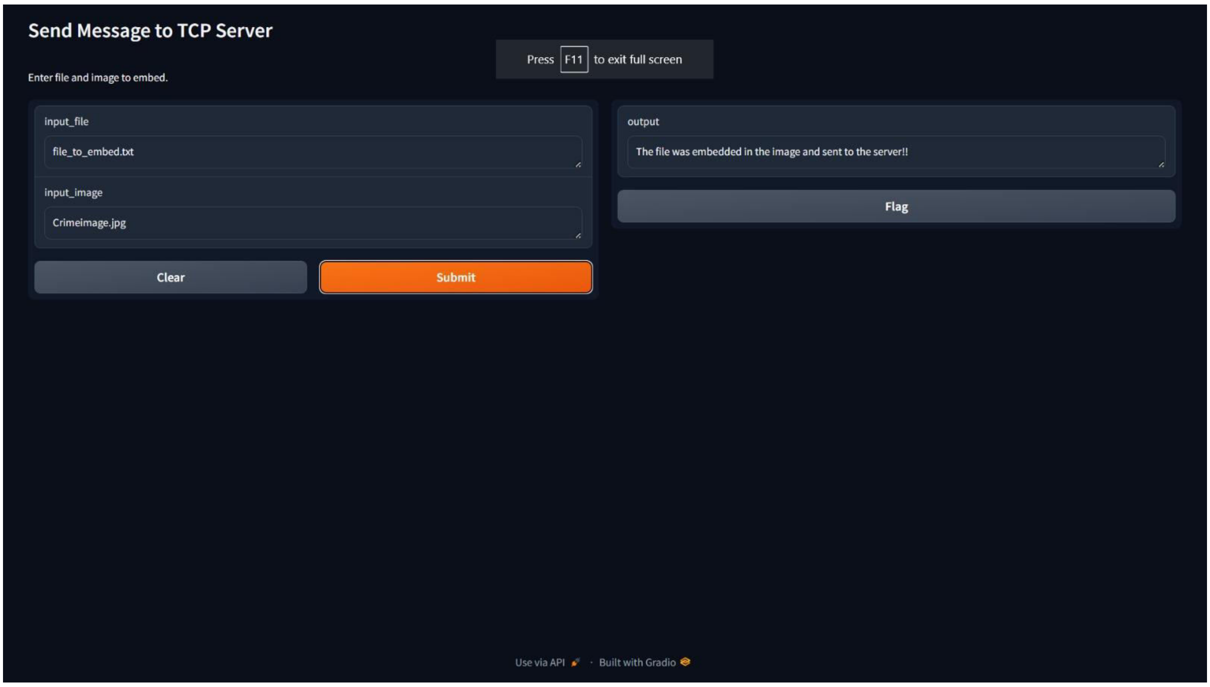
input_file: file_to_embed.txt

input_image: Crimeimage.jpg

output:

Press F11 to exit full screen
Clear
Submit
Flag
Use via API · Built with Gradio

4. SENDING ENCRYPTED IMAGE TO THE SERVER


Send Message to TCP Server

Enter file and image to embed.

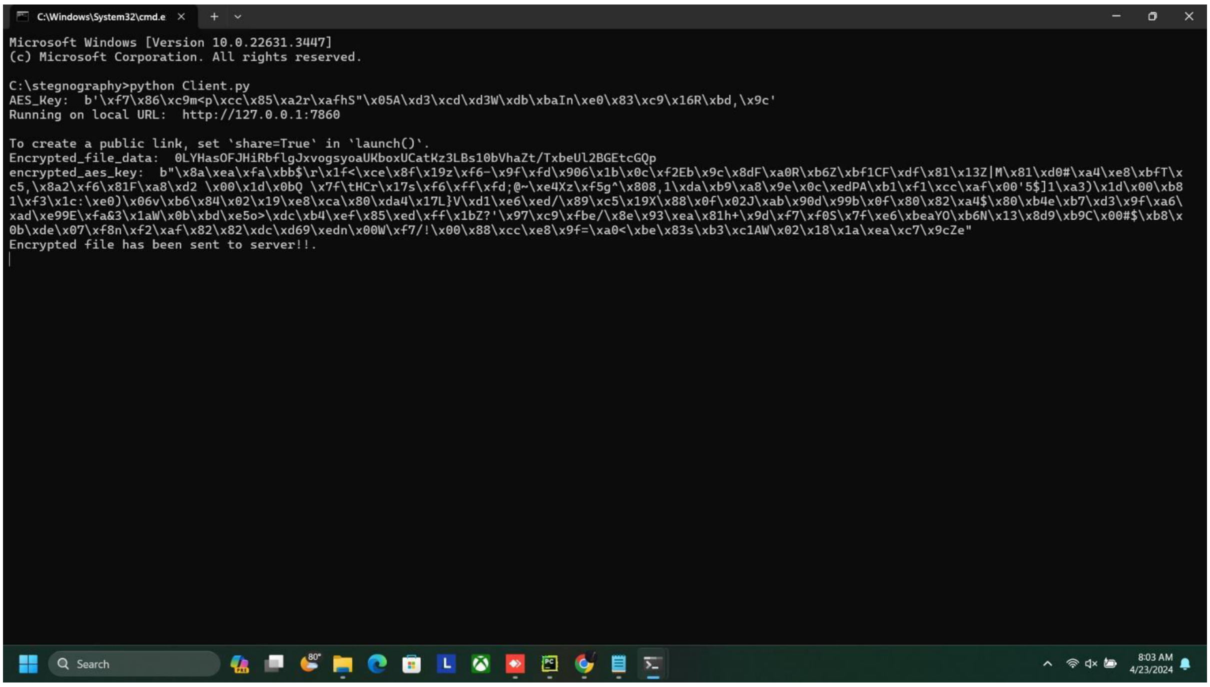
input_file: file_to_embed.txt

input_image: Crimeimage.jpg

output: The file was embedded in the image and sent to the server!!

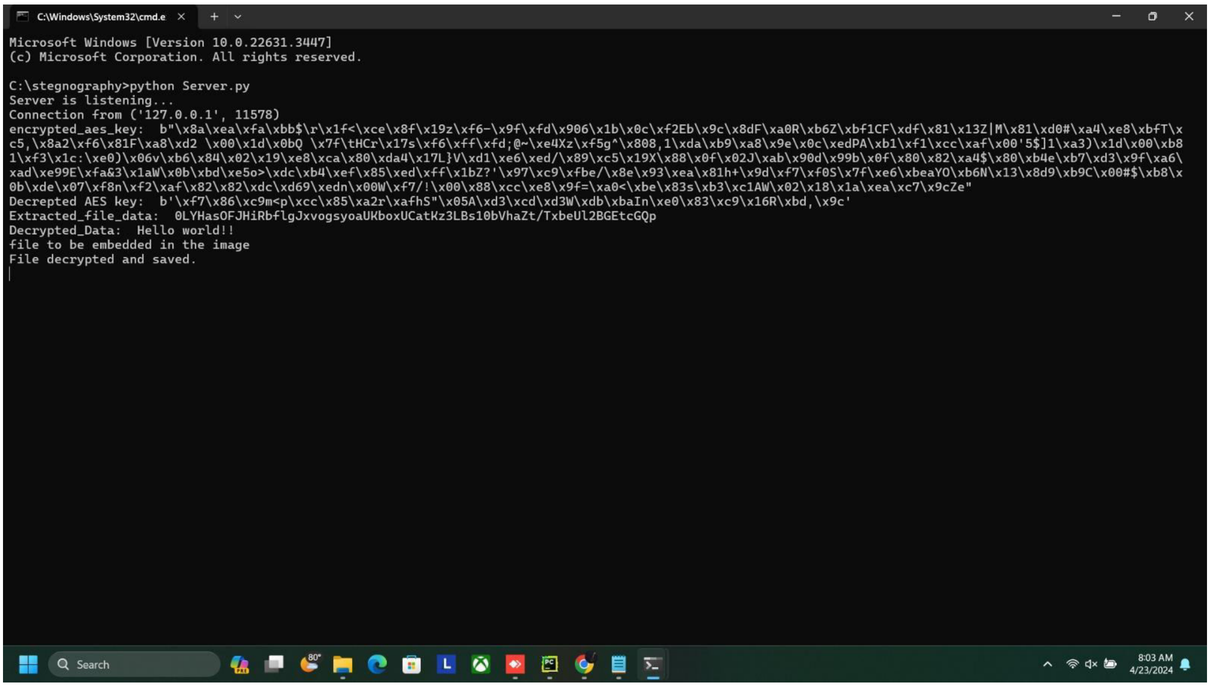
Press F11 to exit full screen
Clear
Submit
Flag
Use via API · Built with Gradio

5. RECEIVED ACKNOWLEDGEMENT IN CLIENT



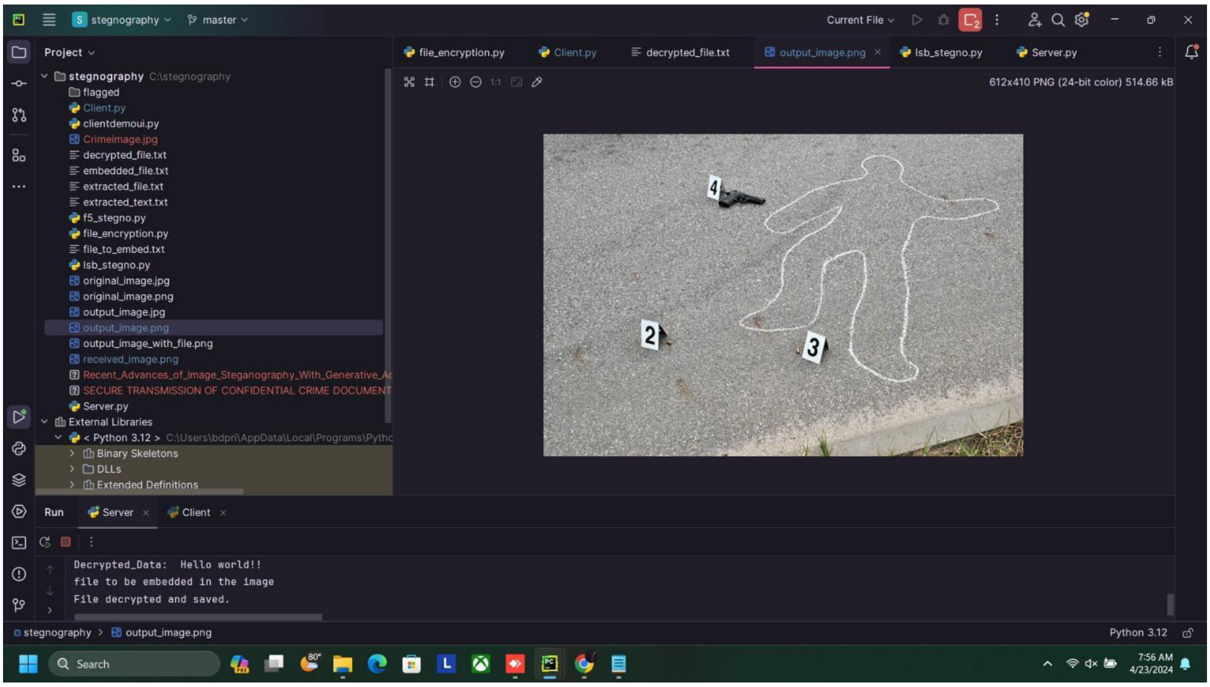
```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\stegnography>python Client.py
AES_Key:  b'\xf7\x86\xc9m<p\xcc\x85\xa2r\xafhS"\x05A\xd3\xcd\xd3W\xdb\xbaIn\xe0\x83\xc9\x16R\xbd,\x9c'
Running on local URL:  http://127.0.0.1:7860

To create a public link, set `share=True` in `launch()`.
Encrypted_file_data:  0LYHasOFJHiRbflgJxvogsyoaUKboxUCatKz3LBs10bVhaZt/TxbeUl2BGEtcGQp
encrypted_aes_key:  b"\x8a\xea\xfa\xbb$\r\x1f<\xce\x8f\x19z\xf6-\x9f\xfd\x906\x1b\x0c\xf2Eb\x9c\x8dF\xa0R\xb6Z\xbf1CF\xdf\x81\x13Z|M\x81\xd0#\xa4\xe8\xbfT\x
c5,\x8a2\xf6\x81F\xa8\xd2 \x00\x1d\x0bQ \x7f\tHCr\x17s\xf6\xff\xfd;@~\xe4Xz\xf5g^\x808,1\xda\xb9\xa8\x9e\x0c\xedPA\xb1\xf1\xcc\xaf\x00'5$]1\xa3)\x1d\x00\xb8
1\xf3\x1c:\xe0)\x06v\xb6\x84\x02\x19\xe8\xca\x80\xda4\x17L}V\xd1\xe6\xed/\x89\xc5\x19X\x88\x0f\x02J\xab\x90d\x99b\x0f\x80\x82\xa4$\x80\xb4e\xb7\xd3\x9f\xa6\
xad\xe99E\xfa&3\x1aW\x0b\xbd\xe5o>\xdc\xb4\xef\x85\xed\xff\x1bZ?'\x97\xc9\xfbe/\x8e\x93\xea\x81h+\x9d\xf7\xf0S\x7f\xe6\xbeaYO\xb6N\x13\x8d9\xb9C\x00#$\xb8\x
0b\xde\x07\xf8n\xf2\xaf\x82\x82\xdc\xd69\xedn\x00W\xf7/!\x00\x88\xcc\xe8\x9f=\xa0<\xbe\x83s\xb3\xc1AW\x02\x18\x1a\xea\xc7\x9cZe"
Encrypted file has been sent to server!!.
```

6.RECEIVED ACKNOWLEDGEMENT IN SERVER



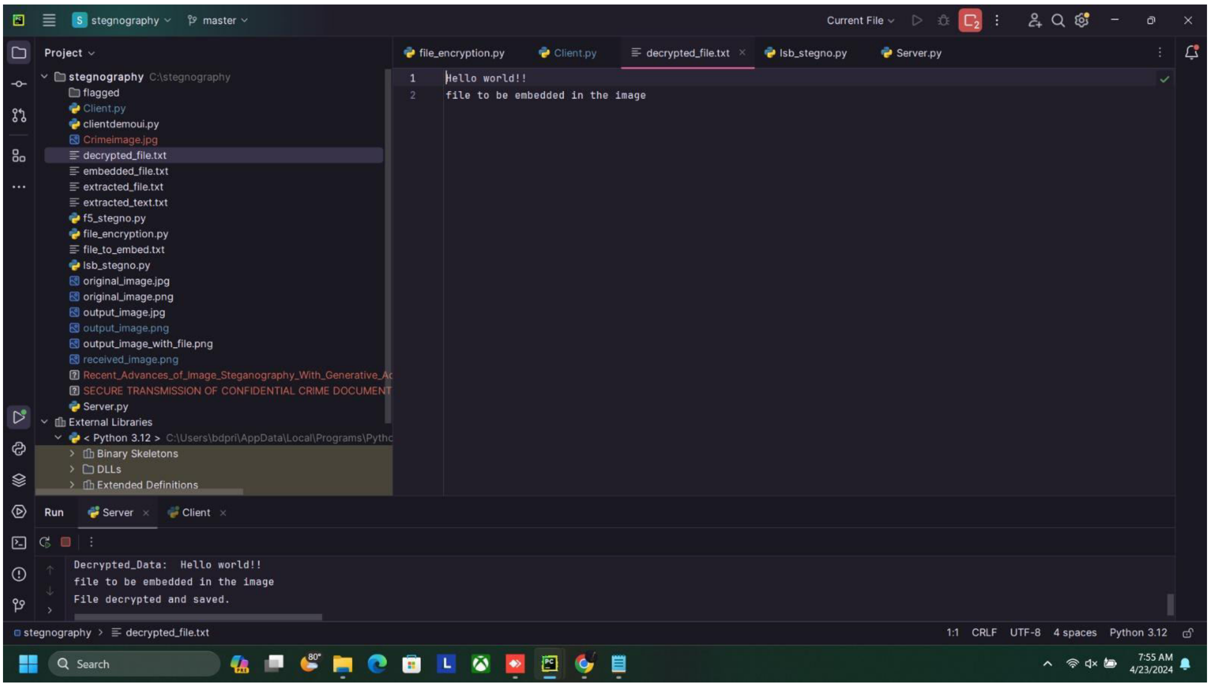
```
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

C:\stegnography>python Server.py
Server is listening...
Connection from ('127.0.0.1', 11578)
encrypted_aes_key:  b"\x8a\xea\xfa\xbb$\r\x1f<\xce\x8f\x19z\xf6-\x9f\xfd\x906\x1b\x0c\xf2Eb\x9c\x8dF\xa0R\xb6Z\xbf1CF\xdf\x81\x13Z|M\x81\xd0#\xa4\xe8\xbfT\x
c5,\x8a2\xf6\x81F\xa8\xd2 \x00\x1d\x0bQ \x7f\tHCr\x17s\xf6\xff\xfd;@~\xe4Xz\xf5g^\x808,1\xda\xb9\xa8\x9e\x0c\xedPA\xb1\xf1\xcc\xaf\x00'5$]1\xa3)\x1d\x00\xb8
1\xf3\x1c:\xe0)\x06v\xb6\x84\x02\x19\xe8\xca\x80\xda4\x17L}V\xd1\xe6\xed/\x89\xc5\x19X\x88\x0f\x02J\xab\x90d\x99b\x0f\x80\x82\xa4$\x80\xb4e\xb7\xd3\x9f\xa6\
xad\xe99E\xfa&3\x1aW\x0b\xbd\xe5o>\xdc\xb4\xef\x85\xed\xff\x1bZ?'\x97\xc9\xfbe/\x8e\x93\xea\x81h+\x9d\xf7\xf0S\x7f\xe6\xbeaYO\xb6N\x13\x8d9\xb9C\x00#$\xb8\x
0b\xde\x07\xf8n\xf2\xaf\x82\x82\xdc\xd69\xedn\x00W\xf7/!\x00\x88\xcc\xe8\x9f=\xa0<\xbe\x83s\xb3\xc1AW\x02\x18\x1a\xea\xc7\x9cZe"
Decrepted AES key:  b'\xf7\x86\xc9m<p\xcc\x85\xa2r\xafhS"\x05A\xd3\xcd\xd3W\xdb\xbaIn\xe0\x83\xc9\x16R\xbd,\x9c'
Extracted_file_data:  0LYHasOFJHiRbflgJxvogsyoaUKboxUCatKz3LBs10bVhaZt/TxbeUl2BGEtcGQp
Decrypted_Data:  Hello world!!
file to be embedded in the image
File decrypted and saved.
```

7. RECEIVED ENCRYPTED IMAGER



```
Decrypted_Data:  Hello world!!
file to be embedded in the image
File decrypted and saved.
```

8.ENCRYPTED FILE



```
Hello world!!
file to be embedded in the image
```

```
Decrypted_Data:  Hello world!!
file to be embedded in the image
File decrypted and saved.
```

VI. CONCLUSION

In conclusion, the proposed system presents a robust approach to secure file transmission within a client-server architecture. By integrating AES and RSA encryption algorithms with LSB steganography, the system ensures confidentiality, integrity, and covert transmission of sensitive data. AES encryption provides strong cryptographic protection for the files, while RSA encryption facilitates secure key exchange between the client and server. LSB steganography adds an additional layer of concealment by embedding encrypted data within carrier files, enhancing the security of transmission. However, it's essential to consider performance implications, key management, and steganalysis techniques to ensure the effectiveness and reliability of the system. Overall, the proposed system offers a comprehensive solution for secure file transmission in networked environments.

REFERENCES

1. Hussain M, Ainuddin WB, Abdul W, Mohd Yamani IBI, Anthony TS. HO, Ki-Hyun J, Image Steganography in Spatial Domain: A Survey. J. Signal Processing: Image Communication, Vol.65, 2018, pp. 46-66.
2. Kamaldeep J, Gill S, and Yadav R, A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the GrayScale Image. J. Comp. Netw. and Communic, 2018, 9475142:1-9475142:10.
3. Lifang Y, Yao Z, Rongrong N and Ting L. 2010. Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm. Eurasip J. Advances in Signal Processing, 2010:876946.
4. Ratnakirti R, Changder S, Sarkar A, Narayan CD, Evaluating Image Steganography Techniques: Future Research Challenges. Proc. Intl. Conf. Comp. Mgmt Telecomm. Vietnam, Jan. 21-24 2013, pp. 309-314.
5. Sabry S. Nassar NM, Ayad,HM, Kelash HS, El-sayed,MA. M. El-Bendary,Fathi E. Abd El-Samie, Osama SF, Secure Wireless Image Communication Using LSB Steganography and Chaotic Baker Ciphering. Wireless Personal Communications, Vol. 91, 2016, pp. 1023–1049.
6. Asha Durafe, A Review of Digital Steganography Methods, Intl. Journal of Creative Research and Thoughts, Vol.5(4), 2017, pp.1129-1134.
7. Patidar, V., Pareek, N. K., Purohit, G. & Sud, K. K. [2011] “A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption,” Optics Communications 284, 4331-4339.
8. Shannon, C. E. [1949] “Communication theory of secrecy systems,” Bell System Technical Journal 28, 656-715.
9. Nassar, Sabry S. Ayad, Nabil M.Kelash, Hamdy M.El-sayed, Hala S.El-Bendary, Mohsen A.M.Abd El-Samie, Fathi E.Faragallah, Osama S.Secure Wireless Image Communication Using LSB Steganography and Chaotic Baker Ciphering, Intl. Journal of Wireless Personel communications, 2016, pp.1024-1049
10. Xin Zhou, Xiofei Tang, Research and Implementation of RSA algorithm for encryption and decryption, Proceedings of 2011 6th International Forum on Strategic Technology, IEEE, 2011, pp. 1118-1121

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details