

Advanced System for Secure Military Communication Using Image Steganography and Block-Rotary Encryption

Malavika V¹, Vinish A², Dr. Shaji B³, Dr. Justin Jose⁴

¹Student, Computer Science Engineering, Nehru College of Engineering and Research Centre, Kerala

²Assistant Professor, Computer Science Engineering, Nehru College of Engineering and Research Centre, Kerala

³Associate Professor, Computer Science Engineering, Nehru College of Engineering and Research Centre, Kerala

⁴Professor, Computer Science Engineering, Nehru College of Engineering and Research Centre, Kerala

Abstract

This project offers a thorough security framework for safe military data transfer, including face recognition, block-rotary encryption, and image steganography to protect private data. Block-rotary encryption further secures the buried data by jumbling it with a secret key, while picture steganography hides data within image pixels, rendering it invisible to the human eye. Face recognition is used for multi-factor authentication to improve security, requiring soldiers to use facial recognition to confirm their identification. Administrators, Departments, and Soldiers are among the user roles that the system offers; each has specific access requirements and features. While departments supervise soldiers and decode vital information, administrators control accounts and deal with data decryption. Sensitive information can be safely exchanged and encoded by soldiers. The system offers a strong solution for secret and safe military communication by fusing cutting-edge encryption techniques with role-based access control, biometric authentication, and data secrecy. The suggested solution responds to the increasing demand for secure communication in military operations by providing a tiered security strategy. It guarantees that sensitive data is hidden and shielded from unwanted access during transmission by fusing steganography, encryption, and biometric authentication. While block-rotary encryption adds another layer of complexity that prevents decryption without the right key, image steganography enables the secret embedding of data within common images. By ensuring that various users, including administrators, departments, and soldiers, have the proper access privileges according to their duties, role-based access management reduces the possibility of data breaches. All things consider, this system offers a very safe, comprehensive way to protect military communications from possible dangers.

Keywords: Steganography, Block-rotary encryption, face recognition, decryption

1. Introduction

Secure and secret communication channels are more important than ever in the quickly changing military environment of today. The safeguarding of secret information becomes crucial to ensuring mission success and crew safety as military operations depend more and more on digital technology. Protecting sensitive

data while it is being transmitted is a difficult task that calls for strong, multi-layered solutions due to the rise in cyberthreats and the possibility of data breaches. By integrating cutting-edge security technologies—image steganography, block-rotary encryption, and face recognition—into a unified system intended to protect vital communication lines, this project tackles the requirement for secure military data transfer.

A key component of this method is image steganography, which makes it possible to hide private information inside of common photographs. Using this method, data is concealed within an image's pixel values, rendering it invisible to the naked eye. Steganography is also a perfect technique for military communications due to its clandestine nature, which enables data to be sent without attracting notice or arousing suspicion. The integrity and secrecy of the data are guaranteed since, even in the event that the image is intercepted, the hidden data cannot be discovered without the right decryption techniques.

Block-rotary encryption is used to add an additional degree of security to the stealth that steganography offers. With this encryption method, data is divided into fixed-size blocks that are subsequently "rotated" or rearranged using a secret key. Even if the secret data is found, illegal access is prevented since the jumbled data cannot be read without the right key. This technique offers a two-pronged defense against unwanted access by combining steganography with encryption to guarantee that military communications are not only concealed but also safe from possible enemies.

Administrators, Departments, and Soldiers are among the user roles that the system is made to accommodate; each has distinct duties and access rights. While departments have control over soldiers and access to vital information, administrators can manage user accounts, decrypt data, and supervise system operations. Conversely, soldiers have the authority to encrypt and safely send private information, guaranteeing that only those who are permitted can access it. The system offers a strong and adaptable solution for secure military communication by fusing these cutting-edge security techniques with role-based access control, protecting the confidentiality, integrity, and authenticity of vital data during the course of its lifecycle. This system's security design also places a strong emphasis on thorough key management, which is necessary to preserve the integrity and confidentiality of encrypted data. Safely handling cryptographic keys is essential in a military setting where a data breach could have disastrous results. Soldiers can request keys when necessary to decode shared data, and the system makes sure that only authorized persons receive decryption keys. By limiting who has access to sensitive communications, this procedure helps reduce the possibility of key exposure or misuse. An essential component of this multi-layered security strategy is effective key management, which facilitates data encryption and decryption while preserving data confidentiality.

The system's capacity to uphold confidentiality and access control during the communication process is another important characteristic. The system makes sure that only authorized users have access to particular data sets and operations by putting role-based access control (RBAC) into place. This is done according to the users' roles within the company. While departments can supervise troops and decrypt pertinent data, they are not given full administrative capabilities. Administrators, on the other hand, have complete access to all data and are able to manage both departments and soldiers. In turn, soldiers are able to safely share and encrypt data with their peers, but they are unable to access sensitive information outside their assigned scope. By guaranteeing that people only have access to the data necessary for their jobs, this hierarchical access structure offers a balanced approach to security.

Operational effectiveness also depends on the system's capacity to securely handle and transfer important information. In military operations, time is of the essence, and the success of the mission depends on

secure communication channels that function swiftly and effectively. Steganography and encryption combined offer a simplified way to send private information without sacrificing security or speed. Soldiers and other staff may send and receive vital information rapidly thanks to the system's low latency, which also ensures a high level of security during the transmission process. Because of its speed and effectiveness, the system is not only safe but also useful for actual military operations.

In summary, this project offers a highly advanced and secure military data transfer technology. The system makes sure that private information is hidden, encrypted, and shielded from unwanted access by incorporating state-of-the-art technologies like multi-factor authentication, block-rotary encryption, image steganography, and face recognition. Additional security layers are added via role-based access control, key management, and user authentication to guarantee that only individuals with permission can access vital data. This all-encompassing, multifaceted strategy provides a strong foundation for protecting military communications, allowing for the efficient, secret, and safe transfer of critical information at all operational levels.

2. Methodology

This approach combines cutting-edge technology like face recognition, block-rotary encryption, and image steganography to produce a reliable system for military data transfer.

2.1. Module 1: Uploading the Images and Sensitive Text

Uploading the necessary resources the sensitive text data, the cover picture, and the key image—is the first stage in the procedure. The base image on which the encrypted data will be concealed is the cover image. The key image serves as a source for the creation of an encryption key, directing the processing of the data and including crucial pixel data. The message that will be encrypted and concealed under the cover image is the sensitive text, which may contain military information or any other private information. Making sure the sensitive data is prepared for encoding and that the photos are uploaded in the correct formats is the first step in the procedure.

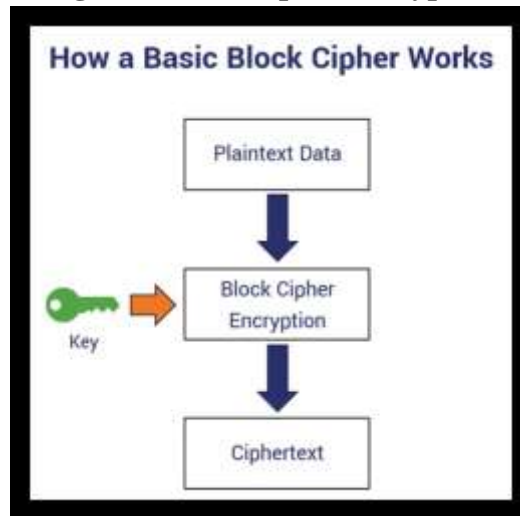
2.2 Module 2: Key Extraction from Key Image

The next step is to extract the pixel values from the key image after the photographs have been submitted. An array-based encryption key is created using these pixel values. The block-rotation encryption pattern used for the sensitive data will be decided by this key array. The encryption process is based on the pixel values of the key image, and the arrangement of these values is essential to guaranteeing that the encryption is secure and distinct. This key array is essential to the system's overall security since it determines how the data blocks will be split up and rotated during the encryption phase.

2.3 Module 3: Block-Rotary Encryption

The sensitive text data is divided into fixed-size blocks, each of which will undergo encryption. The block-rotary encryption method involves rotating the blocks of data according to the key array derived from the key image. For each block of data, a rotation process is applied, where the data is shifted by a number of positions specified by the corresponding pixel value in the key array.

Figure:1 Block cipher encryption



This scrambling process ensures that the original data is thoroughly concealed and cannot be reconstructed without the decryption key. By breaking the data into blocks and applying a rotational shift, the encryption becomes more complex, adding an extra layer of security. Once all the blocks have been encrypted through this rotation process, they are prepared for embedding in the cover image.

2.4. Module 4: Hiding Encrypted Data Using Steganography

The next step is to use image steganography to conceal the encrypted data inside the cover image. This is accomplished by embedding the encrypted data in the least significant bits of the cover image's pixel values using the least significant bit (LSB) approach. The integrity of the image is preserved via the LSB approach, which modifies the pixel values just enough to conceal the encrypted message without producing any obvious deformation. To make sure the secret message is invisible to anyone who might intercept the image, the encrypted data is successively inserted into the image's pixel values. The pixel values are altered such that the hidden information can only be discovered by the recipient who is skilled in data extraction.

2.5. Module 5: Sending the Image

The cover picture is delivered to the receiver after the encrypted data has been integrated within it. It will seem like a normal, unaltered image to any outside spectator, making it very difficult for anyone to notice that it contains important information concealed away. Steganography and encryption work together to protect the message's contents from prying eyes while it is in transit, ensuring the security of data transfer.

2.6. Module 6: Receiver's Side (Decryption Process)

The recipient starts the decryption procedure as soon as they receive the cover image. The key array is first extracted from its pixel values using the key image, which ought to have been safely shared earlier. The block-rotary encryption is then reversed using this key array. The recipient reconstructs the original blocks of encrypted text after extracting the encrypted data concealed in the image's least important pixel segments. Following the extraction of the encrypted blocks, each block is subjected to the opposite rotation procedure, which uses the key array to rotate the blocks back to their initial locations. By restoring the original communication, this decryption procedure enables the recipient to recover the supplied sensitive information.

2.7. Module 7: Face Recognition for Authentication

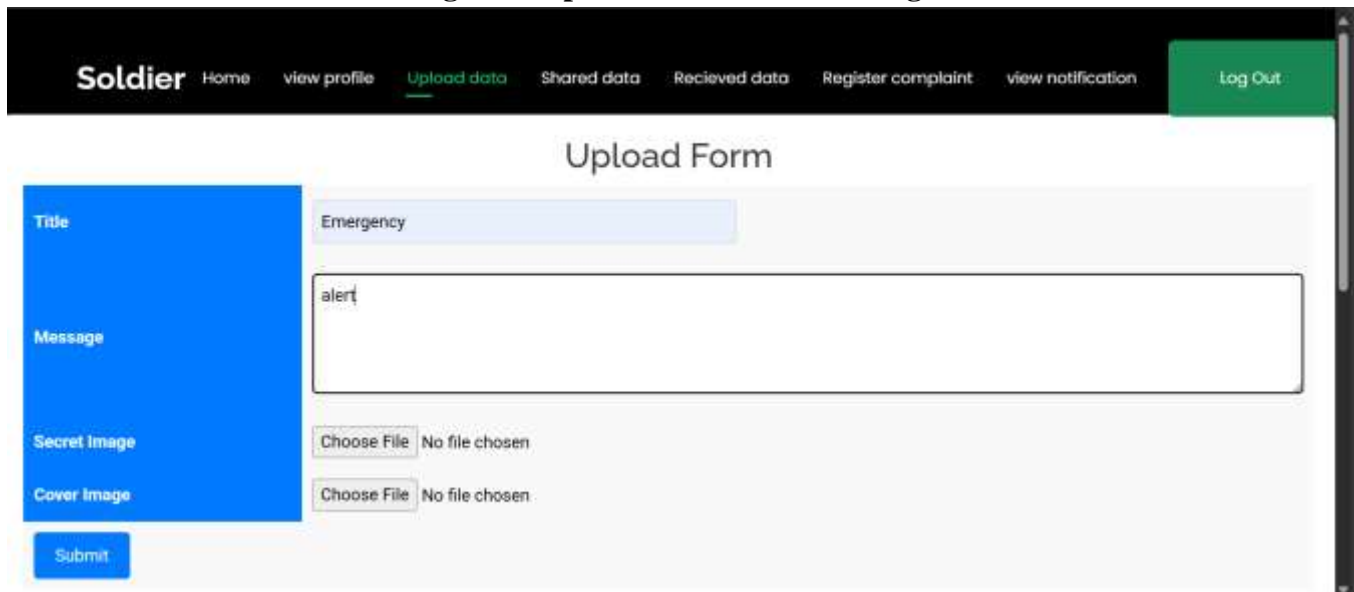
Face recognition technology is incorporated into the system to guarantee that only authorized individuals

can access and utilize it. During the login procedure, face recognition is used as an authentication method. A user's identity is confirmed by capturing their face characteristics and comparing them with the biometric data that has been stored when they try to access the system. By guaranteeing that only authorized soldiers, administrators, or department heads may access and use the system, this biometric security feature provides an extra degree of protection and stops unauthorized access to important data.

3.Results and Discussions

Promising outcomes from the Military Data Transfer Using Image Steganography and Block-Rotary Encryption study showed how well cutting-edge technology may be integrated to guarantee the safe and discrete transfer of critical military data. Without significantly altering the cover image's visual look, the encrypted data was successfully concealed within it thanks to the image steganography methodology, more especially the Least Significant Bit (LSB) method. Because the changed pixel values were invisible to the human eye, this made guaranteed that the private information would not be discovered by unauthorized parties. For military applications where preserving the security and integrity of the data while it is being transmitted is crucial, this secret data embedding technique is perfect. The system's security was further improved by the implementation of block-rotary encryption.

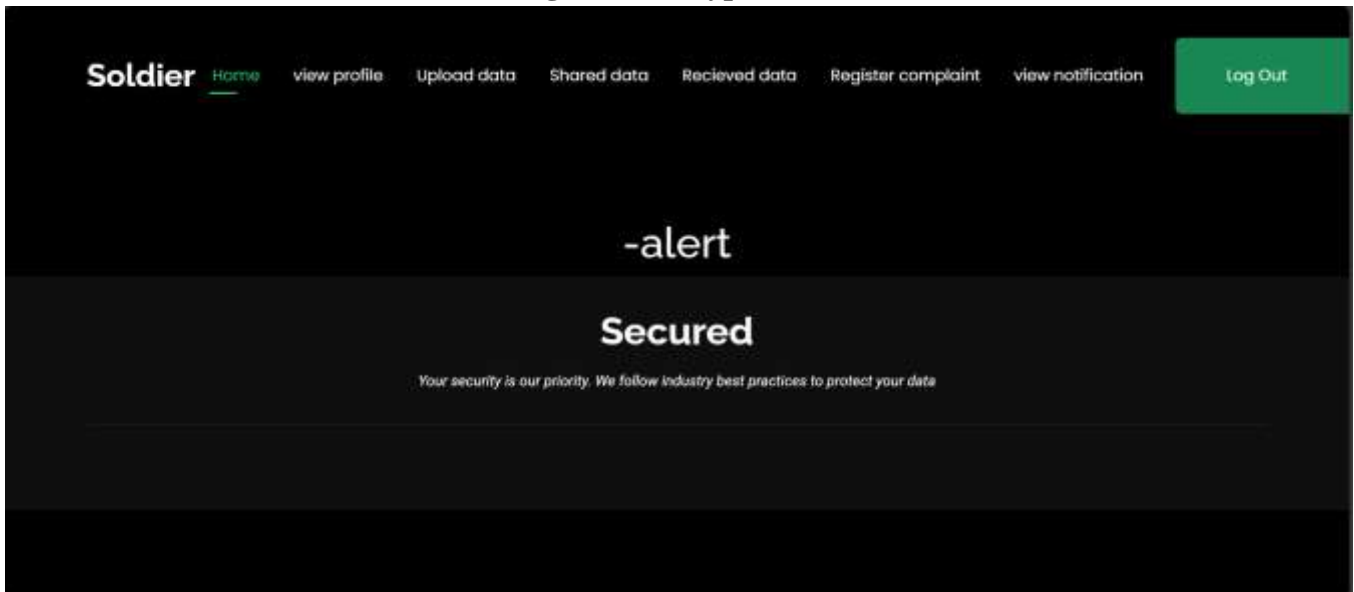
Figure:2 Upload secret text and images



The screenshot shows a web application interface for a user named 'Soldier'. The navigation bar includes links for Home, view profile, Upload data (highlighted), Shared data, Recieved data, Register complaint, view notification, and Log Out. The main content area is titled 'Upload Form' and contains a vertical sidebar with labels: Title, Message, Secret Image, and Cover Image. The form fields are: Title (text input with 'Emergency'), Message (text area with 'alert'), Secret Image (file upload with 'Choose File' and 'No file chosen'), and Cover Image (file upload with 'Choose File' and 'No file chosen'). A blue 'Submit' button is located at the bottom left of the form.

To make the data unintelligible without the decryption key, the sensitive text was divided into fixed-size blocks and rotated according to a key array that was created from the pixel values of the key image. By adding a layer of complexity, this encryption technique made it difficult for anyone intercepting the transmission to quickly recreate the original data. The encryption procedure was successfully tested, and the original sensitive message was precisely restored by error-free decryption.

Figure:3 Decrypted text



Face recognition, another essential system component, shown remarkable efficacy in safeguarding system access and preventing unwanted users from accessing or altering the data. Only authorized people were able to log in and perform tasks like encoding, decoding, and exchanging sensitive information thanks to the facial recognition system's effective and precise user authentication. By adding an additional layer of security, this biometric authentication method decreased the possibility of criminal activity or illegal access.

Face recognition, block-rotary encryption, and image steganography were used to create a strong system that safely sent data without leaving it open to illegal access or interception. To an outside viewer, the transmitted cover image which held the secret encrypted message looked like any other image. By keeping the communication private while in transit, this visual inconspicuousness made the data transfer procedure safe. However, the accuracy of the face recognition system and the strength of the encryption key are crucial to the system's security. The data's security might be in jeopardy if one of these elements were compromised since an attacker might be able to get the decryption key or get past the authentication procedure. Project's outcomes demonstrate the potential of employing this integrated strategy for safe communication in military settings. Steganography and encryption work together to make sure that data is safely jumbled and buried, making it nearly impossible for unauthorized people to read or decrypt it without the right key. Future developments might concentrate on enhancing the system's scalability so that it can manage higher data volumes and improving the encryption techniques for even more robust security. To guarantee that access is only given to authorized persons, more work could be done to improve the face recognition system's speed and accuracy as well as its resistance to spoofing or false acceptance. All things considered, this research has effectively illustrated a very safe way to send sensitive military data, which may find use in actual military communications where data integrity and confidentiality are crucial.

4. Conclusion

To sum up, the project effectively illustrates a novel and safe framework for sending classified military data. Through the integration of face recognition, block-rotary encryption, and image steganography, the system maintains the covert aspect of the connection while guaranteeing that data is secure and confidential during transmission. When these technologies are combined, a strong method for concealing

encrypted data under a cover image is created, making it practically hard for unauthorized parties to find or access the data. The data is further shielded from decryption without the right key by the additional layer of difficulty added by the block-rotary encryption method. By providing a safe and dependable authentication procedure that guarantees that only authorized personnel can access the system, the face recognition component fortifies the system. Even if the project's goals are met, it can still be improved in the future to increase scalability, optimize encryption algorithms, and improve the facial recognition system for even higher security and effectiveness. At the end of the day, this project offers a strong basis for safe military communication and shows how cryptography and biometric security may be used to protect sensitive data in high-stakes situations.

References

1. M. M. Abu-Faraj, K. Aldebei, and Z. A. Alqadi, "Simple, efficient, highly secure, and multiple purposed method on data cryptography" *Traitement du Signal*, vol. 39, no. 1, pp. 173–178, Feb. 2022.
2. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A complex matrix private key to enhance the security level of image cryptography" *Symmetry*, vol. 14, no. 4, p. 664, Mar. 2022.
3. A. Sharma and R. Kumar, "Performance and security analysis of block ciphers in mobile communication" *Int. J. Mobile Commun.*, vol. 20, no. 1, pp. 40–53, 2022.
4. P. Kumar, S. Raj, and M. Patel, "Enhancing security in data transmission using block cipher algorithms and steganography" *IEEE Access*, vol. 10, pp. 12045–12059, 2022.
5. S. Batra and D. Singh, "Security of AES block cipher and its applications in cloud computing" *IEEE Access*, vol. 9, pp. 10344–10355, 2021.
6. V. Sivasubramanian and S. Ramachandran, "Efficient block cipher-based encryption and decryption algorithms" *Int. J. Comput. Sci. Eng.*, vol. 8, no. 2, pp. 122–130, 2020.
7. W. H. Jeong, B.-G. Yeo, K.-H. Kim, S.-H. Park, S.-W. Yang, J.-S. Lim, and K.-S. Kim, "Performance analysis of the encryption algorithms in a satellite communication network based on H-ARQ," *J. Inst. Webcasting, Internet Telecommun.*, vol. 15, no. 1, pp. 45–52, Feb. 2015.