LOGICAL TECHNIQUES IN COMPUTER SCIENCE
Open Journal

Review

Enhancing Image Cryptography Performance with Block Left Rotation Operations

Mohammad S. Al-Batah[1*]; Mowafaq S. Alzboon[1]; Mazen Alzyoud[2]; Najah Al-Shanableh[2]

[1]*Department of Computer Science, Faculty of Science and Information Technology, Jadara University, Irbid 21110, Jordan*
[2]*Department of Computer Science, Faculty of Prince Al-Hussein Bin Abdallah II for IT, Al Al-Bayt University, Mafraq 25113, Jordan*

[*]***Corresponding author***
Mohammad S. Al-Batah
Department of Computer Science, Faculty of Science and Information Technology, Jadara University, Irbid 21110, Jordan

Article information
Received: February 16th, 2024; **Revised:** May 3rd, 2024; **Accepted:** May 29th, 2024; **Published:** June 9th, 2024

Cite this article
Al-Batah MS, Alzboon MS, Alzyoud M, Al-Shanableh N. Enhancing image cryptography performance with block left rotation operations. 2024; 2(1).
doi: https://doi.org/10.70705/ppp.ltcs.2024.v02.i01.pp39-47

ABSTRACT

Both long and short text messages are sent and received over a variety of platforms in today's linked world. It is becoming more important to protect communications from possible dangers like intruders, abusers, and data hackers due to the increasing amount of sensitive and specialized information being sent. In order to simplify data security processes and simultaneously resist hacking efforts, this research presents a novel technique. The heart of this approach is based on using a complex variable content private key that allows for easy editing without affecting the security of encryption and decryption. Crucially, this private key is generated using a covert color picture, which the sender and recipient are obligated to securely keep. The private key may automatically adjust to fit the length of the secret message by using a chosen color picture. Segmenting the communication into blocks of preset sizes, with the sender and receiver working together to establish these parameters, is advised to strengthen the degree of security. Then, according to what the parties involved in the communication have agreed upon, the bytes in each block are combined into one vector and then rotated to the left by a certain number of bits. The use of a variety of color pictures and text messages allows for the empirical validation of the suggested technique. By comparing it to current approaches, we can see that the suggested methodology is far more effective and resilient, which proves that it represents a substantial paradigm shift in data security.

INTRODUCTION

Security and efficiency have been the primary goals of recent cryptographic developments. In order to encrypt hidden data, this research presents a new cryptographic technique that makes use of block rotation left operations and their intrinsic mathematical features. Our solution uses simpler but effective rotational transformations to alter data blocks, unlike existing approaches like DES, AES, or Blowfish that depend on sophisticated substitution and permutation networks.

Several distinct benefits are offered by block rotation left procedures. To begin with, they need less computing power and are perfect for settings with low processing capacity since they need less resources. Second, real-time applications rely on the predictable nature of rotational shifts to provide a high-speed operation. To further complicate linear and differential cryptanalysis assaults, the approach adds an additional layer of protection via obfuscation when paired with modular adding and binary XNOR operations as defined.

Despite their robustness, traditional cryptographic methods may be inefficient when it comes to processing massive amounts of data rapidly and can incur substantial computing overheads. On the other hand, our suggested approach improves throughput by taking advantage of the speed and simplicity of block rotations.

during cryptographic processes, thereby lowering their latency. This makes it an ideal choice for real-time communications and streaming services, which both need fast encoding and decoding, as well as for safeguarding data on high-speed networks.

You may immediately address the comments for greater clarity and justification in your exposition by emphasizing on these factors in the introduction. This will effectively set the tone for discussing the proposed cryptographic approach and its comparative merits over current methods.

2.**DUC**Related Work

A Block Cipher-based security method is currently under development, which will use binary XNOR operations for encoding and decoding, as well as modular addition and rotating shift operations. The initial data transmission is a series of bits, which are then partitioned into blocks of size s. Examples of values for s that are powers

of three include 3, 9, 27, 81, and 243. The addition of zeros at the most significant bit (MSB) site guarantees that each block has an odd number of bits [1]. There are two steps to the encryption procedure. The initial step is to add adjacent blocks using a modulus of 2s in a modular fashion. This procedure updates the block that comes after it while keeping the first block unaltered. The MSB gets rid of any carry that is formed during the summing process. Phase two involves obtaining the encrypted text by rotating the output stream left and right bits and then performing a logical XNOR operation. Blocks having dimensions between 3 and 3n may be treated using this method. Decryption involves using modular decryption and inverting the sequence of operations.

In this age of social media and possible data breaches, we presented an easy and effective approach to message cryptography to solve the problem of safe message protection [2]. The approach requires segmenting the message into predetermined chunks with sizes between two and sixty. The number of rotation digits for the corresponding block during the block rotation left operation is determined for each element in a private key array that is generated from a secret color picture. The efficiency of the suggested technique is assessed using parameters such as throughput, correlation coefficient (CC), peak signal-to-noise ratio (PSNR), and mean square error (MSE). Some of the most popular message encryption algorithms are compared, such as Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF). Because the suggested technique makes use of a secret picture, a fixed block size, and computed Rotation Left Digits (RLD) for every block, experimental findings show that it is both secure and effective.

An innovative and user-friendly approach to data encryption securely transmit important, private, and secret communications. One set of private keys is used for XORing operations, while the other set is used for rotation to the right of each byte. The suggested approach generates these keys using two image keys. For security reasons, we keep the image keys secret. The technique makes use of two hidden variables—the block size and the number of rounds—that may be changed. Carrying out the procedure entails different messages, ranges of block sizes, and cycles [3]. The results will be compared to those of DES to show that the suggested approach can keep throughput high even when block size and round count increase.

It tackles the critical problem of preventing hackers from gaining access to secret communications. We provide a straightforward and versatile data cryptography system that can encrypt and decode messages of any length and both grayscale and color pictures. This approach makes use of a private key that stores all the data needed to generate keys that are inherently chaotic. Index keys, derived from these keys, are used as a lookup table throughout the encryption and decryption processes. To protect against assaults, the produced key has a complicated structure and a vast key space, and it is very sensitive to the contents of the private key. Multiple test analysis techniques will be used to examine the outcomes once the suggested approach is implemented utilizing different messages [4]. The proposed approach will be tested in both the encryption and decryption stages using quality analysis, which measures MSE, PSNR, CC, and NSCR values.

By highlighting the method's vulnerability to the chosen private key, a sensitivity analysis prevents the decryption process from progressing smoothly and instead treats any modifications as hacking efforts, leading to a corrupted message. The effectiveness of the suggested approach will also be shown by a speed analysis, which will compare the findings to other methods to show the speedup.

A large number of data encryption techniques, including those based drawbacks of DES include a fixed block size, a predetermined private key length, the need for many rounds, and possible security holes. The purpose of this research article is to provide a novel approach to secret message cryptography that overcomes these shortcomings. Whether your message is short, medium, or large in length, the suggested approach is adaptable and can handle them all. It checks that the quality metrics including peak signal-to-noise ratio (PSNR), correlation coefficient (CC), and mean square error (MSE) are within acceptable limits. The approach generates the necessary private keys for determining the number of rotation digits needed in character rotation using three secret image keys. The suggested method's underlying actions are unaffected by changes to these image keys, adding an extra degree of security [5]. A comparison with DES will be done to show that the suggested strategy is successful. In this comparison, we shall see how the suggested strategy improves upon more conventional methods that rely on DES. Compared to current approaches based on DES, this study intends to deliver improved security, flexibility, and performance by introducing this novel way of secret message cryptography.

Mobile ad hoc networks play an essential role in the ease of driving and the security of traffic. We need a conditional privacy-preserving authentication (CPPA) method to fix VANET security flaws and meet their security criteria. The inability to update the system secret key (SSK) and the high communication and storage overhead are two of the main drawbacks of traditional CPPA methods. Our solution to these problems is an elliptic curve CPPA signature technique. algorithms, guaranteeing very little transmission overhead for urgent communications. Furthermore, we provide a method for updating SSKs that is based on secure pseudorandom functions and Shamir's secret sharing. By reducing storage needs and providing shorter transmission delays than previous techniques, our approach meets privacy and security criteria [6].

There are security risks associated with using visual media data because of how easily it may be altered with modern technologies. Using cryptography may improve the security of transferring visual data. This research made use of the LSB steganography technique and the RC4 (Rivest Code 4) encryption and decryption algorithm. Making interception more difficult by embedding messages into the picture was the purpose of creating a stronger encryption. The findings prove that RC4 and LSB steganography are powerful tools for protecting data requirements and hidden messages in pictures. How many messages need to be encrypted depends on how long it takes to encode and decode them [7].

Current authentication methods that conditionally protect user privacy ways in vehicle ad hoc networks (VANETs) depend on operations that multiply points, which leads to performance overhead. We provide a solution to this problem by use of elliptic curve cryptography (ECC) that relies on point addition operations to authenticate and sign communications. To become registered nodes in VANET, cars in our method join the network, broadcast traffic-related messages,

and get a pseudonym and secret key from a nearby RSU. A successful mutual authentication is shown using Burrows-Abadi-Needham (BAN) logic. Our solution meets all security and privacy standards, according to the formal security study. Our technique achieves a reduction of 99.3% for message signing, 99.7% for individual authentication, and 98.1% for batch authentication, respectively, according to performance assessment, which demonstrates that computation costs are greatly reduced compared to current schemes [8].

The messaging app WhatsApp is compatible with all major platforms.

It provides E2EE encryption to safeguard user data. Whatsapp ensures the privacy and integrity of user-sent communications by using cryptographic techniques including message authentication codes (MACs) and one-time pads (OTPs). Cryptographic services are becoming more important in the corporate sector, as shown by the introduction of E2EE. These services not only contribute to a prospective company strategy but also have long-term ramifications. With an emphasis on privacy and security, WhatsApp shows that it is serious about protecting its users' information and conversations [9].

The main objective of using voice encryption is to protect sensitive conversation information from prying ears. Protecting audio communications requires the use of cryptography and steganography. For audio communications, it examines the Advanced Encryption Standard (AES) algorithm, and for pictures, it examines the Least Significant Bit (LSB) steganography method. The receiver receives the generated stego picture, which is then assessed using measures such as mean the signal-to-noise ratio (PSNR) and the mean square error (MSE). Based on the study results, stego pictures with LSB values of 1 or 2 seem exactly like the original cover image, successfully hiding the concealed sound [10].

The extensive usage of color digital photos in many applications, some of which deal with sensitive personal information, emphasizes the need of protecting these images. We suggest a safe way to keep these pictures and any sensitive information they may contain safe. You may use this approach to protect photos of any size or kind, as well as secret messages of any length. Utilizing two colored pictures to produce secret private keys for encryption and decryption procedures, the suggested approach provides a high degree of security. In order to determine how well the approach works, we look at quality metrics like the correlation coefficient (CC), peak signal-to-noise ratio (PSNR), and mean square error (MSE) while the encryption and decryption processes are underway. To prove how efficient and effective this system is, its practical outcomes are compared to those of established cryptography methods. The goal of the suggested approach is to reduce the time required for encryption and decryption while simultaneously increasing cryptography's throughput. The overarching goal of this study is to meet the requirement for strong security measures in the modern digital environment by developing an efficient and safe way to store color digital photographs and sensitive information [11].

We provide a new approach to encryption and text message decryption, highlighting the need of safeguarding communications of varied lengths. To guarantee the security of the encrypted communication against unwanted access, the suggested approach uses a secret color picture to produce a private key. This approach has been tested and shown to be effective in achieving desirable mean square error (MSE) and peak signal-to-noise ratio (PSNR) values during encryption and decryption. The findings have been published and validated. To determine the performance improvement made by the suggested technique, a comparative study of performance metrics is carried out in comparison to the DES and AES approaches [12].

An easy-to-implement scheme for secret message cryptography is laid forth. The first step is to transform the message into a binary matrix. After that, it is transformed into a matrix with 16 columns. An index key is produced and used to rearrange the elements of this matrix. To create the necessary index key, the private key uses chaotic parameters in conjunction with a chaotic logistic map model to produce a 16-element chaotic key. With the suggested approach, you may encrypt and decode communications of any length, thanks to its versatility. Changing the key or the message has no effect on the method.

Because the encrypted message is very sensitive to the chosen private key, any changes made to it throughout decryption would cause the message to be distorted and unintelligible. The success of the suggested technique will be evaluated by testing and implementing it with messages of different length. The results will show how the approach is sensitive, efficient, and of high quality [13].

When creating an encryption key for a message, selecting a private key is critical. Because part of the encryption time is spent on creating the secret key, this step greatly affects the security and implementation speed of the encryption technique. Making use of a secret index key is one of two methods for working with private keys. The first method creates a secret index key from a chaotic key using a logistic map model that generates chaotic keys. In the alternative method, a secret index key is created by using a color picture as the image key, then extracting an array from the image. To reverse-engineer the binary bits of the message characters, a straightforward encryption-decryption procedure is used, which relies on the secret index key. The two methods for creating the secret index key are tested with different messages and the results are evaluated. The findings from the analysis are used to provide suggestions for the length, security, quality, and speed of the message cryptography [14]. In 1976, public key encryption was introduced, which was a huge step forward for the cryptography sector. This revolutionary development was critical in protecting and verifying communication networks and allowing for the secure delivery of sensitive communications. Furthermore, it prepared the way for new social interactions to form, made possible by communication technologies that are based on the internet. In order to identify a cryptographic revolution, this academic study explores the historical changes that took place in the '60s and '70s. The paper explores historical data to determine how cryptographers came to agree on public key cryptography, drawing attention to the critical need of privacy in light of government monitoring abuses. At a period of great social and political upheaval, cryptography emerged as a unifying strategy for controlling information in an ever-changing technical and political environment. The study deduces from its findings that public key encryption not only

offered a technological solution to the problem of monitoring but also rethought the theoretical underpinnings of cryptography [15].

Protecting the integrity of data in transit is crucial. Because of security concerns, sending confidential information or messages via the Internet is not without its difficulties. Transmitting secret communications in textual form and hiding information are typical uses of cryptography. Steganography is one of the methods that have been created to conceal information in any media. By incorporating multi-image steganography into a secure communication system, the sender and receiver may engage in protected contact, shielded from outside influence. One of the most common ways to hide information is by picture steganography. This technique involves embedding encrypted data, called ciphertext, into an image, called a cover image, so that no one can see it. Covert information may be presented in a variety of formats, including text, photos, audio, and videos. Multi-

To increase the difficulty of data concealment and so deter possible hackers, picture steganography entails separating the secret code into several pieces and inserting them into various cover pictures. When it comes to building a safe and reliable system, this research offers two picture steganography techniques: the Least Significant Bit (LSB) approach and the Advanced Encryption Standard (AES) methodology of cryptography. Using a symmetric key, both the sender and the receiver are able to encrypt and decrypt data in this system [16].

Threats to the security of wireless sensor networks (WSNs) include eavesdropping and flood assaults, both of which may damage sensor equipment and put the network at risk. We present the Token with Secret and Public Keys Sharing (TSP-KS) mechanism, which mitigates the risk of key leaking in WSNs. Cryptography allows for the establishment of secure communication even when malicious actors are present.

Traditional public key cryptosystems provide safe communication without the need for shared secrets between senders and receivers. However, as compared to symmetric key cryptosystems, their performance is sometimes hindered due to their dependence on complex mathematical computations [17]. For example, there are a number of uses where the computationally heavy encryption of long communications using public key cryptography could be problematic. In order to circumvent this drawback, hybrid systems combine the two methods, striking a balance between efficiency and security. Any WSN administrator worth their salt may create a token, private key, public key, and secret key. The sensor devices and administrator use the token as an access control mechanism, and the base station and sensor devices encrypt packets using the secret and public keys. In order to decrypt data, the administrator uses the private key. Tokens, secret keys, and public keys are securely shared between the administrator, the sensor devices, and the base station in order to allow encryption. Tokens, secret keys, and public keys are distributed decentrally to the base station and sensor devices using the TSP-KS algorithm. Results from experiments show that the TSP-KS algorithm is a good choice for safely exchanging tokens in addition to public and secret keys.

Collaboration improves the degree of data security. combining the conventional LSB steganography method with data compression and encryption. Data embedding, compression, encryption, and decryption are some of the security procedures that the suggested technique use to build further levels of concealment. The secret file is encrypted and decrypted using the Vigenere cipher, and the ciphertext is compressed using the Huffman coding technique [18]. Using three different picture carriers with secret messages of 16, 32, and 48 kB in size, we examine the efficacy of the suggested technique. Metrics like peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), stego picture file size, and mean square error (MSE) show that the suggested technology is more imperceptible than typical LSB image stereography.

There are a number of methods used to encrypt digital color photographs, but the most essential and often used one is the Least Significant Bit (LSB) approach. On the other hand, anybody with programming knowledge may decipher the hidden message since the LSB approach is public knowledge. This study's overarching goal is to shore up the LSB method's security and prevent prying eyes from seeing the encoded secret message [19]. A simple method using covert messaging The message will be encrypted using cryptography before being embedded using the LSB technique. Use a scaled color picture as an image key to create a secret private key for encrypting and decrypting the secret message; this approach uses image keys. The message length and the image key you choose will dynamically adjust the private key's length and contents. Only the sender and the recipient will have access to the secret image key, which may be altered at any time. The usefulness of the suggested crypto-steganographic technology in improving the protection of secret communications will be shown by its implementation.

Making sure the LSB approach is secure in data storage writing a biography is crucial. We provide a safe LSB technique that improves the concealment of secret information. Partitioning the cover picture into blocks and selecting one to hide and extract messages is the suggested way. A private key is used for this process. The sensitivity of the retrieved message is affected by the number of blocks used and the size of those blocks [20]. By using a patch approach, which streamlines the operations and enhances overall efficiency, the suggested method streamlines the hiding and extraction procedures. We will do a sensitivity analysis with different pictures and texts to see how well the strategy works. To evaluate how well the process works, we will look closely at the stego pictures that come out of it.

New forms of electronic communication have made it possible to the sharing of data between different entities. But not all information is designed to be shared widely; some may have special goals or need to be kept confidential. Therefore, it is critical to guarantee the security of information. The Vigenere cipher and the Caesar cipher are two examples of the many ways this may be accomplished using cryptography. Methods like this use keywords or changes in character positions to replace each original character with its associated letter or character. Nonetheless, tools like frequency analysis and the brute force approach make short work of such procedures. This study suggests a patch that merges the Vigenere and Caesar ciphers to fix this flaw; the techniques that emerge are then converted into names of chemical elements from the periodic table. Another use of steganography is the concealment of communications or data. It is anticipated that the results of the encryption process would grow more difficult to decipher [21]. Cryptography and steganogra-

phy have a long and storied history have provided ways for certain people, organizations, and governments to convey, hide, and secure sensitive information.

executive branches. These methods include the use of codes that can only be deciphered by the sender and the receiver, whether those codes are embedded in text, graphics, or some other media. The educational, research, and recreational uses of cryptography and shorthand are the focus of this effort. In this case, we're using a manual, randomized technique to fitting each word, which allows us to utilize a basic but en- gaging "game" to transmit encrypted information to particular people or groups. Taking on this air of secrecy prevents unwanted people from discovering the information [22].

We laid up a simple and readily implementable data cryptography approach. This approach can encrypt and decode digital pictures of any size or kind, including secret messages, color images, grayscale images, and more. An easier encryption and decryption mechanism is used to speed up the cryptography process. Rearranging the values of pixels is a simple procedure that this function uses. An index key is created using a chaotic logistic map model using chosen values of chaotic parameters, and then used to accomplish the rearrangement. Incorporating a private key that increases the key space, the suggested solution improves picture protection and makes it more resistant to hacking attempts. The quality, efficiency, and sensitivity of the suggested approach will be shown by testing and implementing it on a variety of photos and then carefully analyzing the results [23]. The field of cryptography deals with the authenticity, integrity, and secrecy of communications during transmission. Cryptosystems that use public and private keys for encryption and decryption are built upon the well-known Diffie-Hellman (DH) key exchange protocol, which allows the sender and the receiver to generate a shared secret key. The man-in-the-middle (MITM) attack, which permits eavesdropping, modification, and interception of the shared secret key, is particularly strong against this protocol [24]. This research aims to solve this problem by suggesting a solution that combines DH key exchange with the public key RSA encryption system. This would make it more resistant to MITM attacks. This technique is evaluated by comparing its performance to that of the RSA Cryptosystem and the DH Key Exchange algorithm.

It is critical to prevent hackers from gaining access to sensitive communications. Traditional symmetric and asymmetric data encryption approaches will be investigated and compared in this research. Additionally, we provide an easy, very safe, and effective way to encrypt private communications. Using a private key with a variable length is fundamental to our method, and we recommend increasing the length to both increase the key space and strengthen defenses against assaults. Because the private key is so crucial to decryption, tampering with the encrypted communication in any way is tantamount to an effort at hacking. Implementing our suggested strategy with varied message sets and subjecting the outputs to extensive evaluation will allow us to gauge its effectiveness.

Investigate, and assess the accomplished degrees of safety, effectiveness, and quality [25].

The need of protecting sensitive information, especially private and secret communications, cannot be overstated. With this study, we have a new method of data cryptography that can encrypt and decode messages of any size. In order to prevent guessing or hacking, the suggested solution uses a complicated private key with five parts that use a double data type. Two secret keys, one generated from an image key and the other from the confidential data, are very vulnerable to changes made to the private key information, no matter how little. The approach uses the chaotic logistic map model to produce the second key, and it handles long messages by splitting them into smaller chunks to improve performance. We will execute the recommended approach and carefully examine its sensitivity, quality, security, and speed to show you how great it is. To test the method's quality, we will calculate quality metrics including MSE, PSNR, and CC. To examine efficiency, we will measure cryptography throughputs, encryption and decryption times. To further demonstrate how sensitive the outputs are, several private keys will be tried throughout the decryption process. To showcase the improvements provided by the proposed methodology, we will compare it to current approaches in an evaluation [26].

3. Research Contribution, Objectives, and Security Strength

Thirdly, the contribution to research. In order to prevent misuse, intrusion, or data hacking, this study seeks to address the need of safeguarding both lengthy and brief text messages. Simplifying data protection while making message compromise difficult for hackers is the major aim. The presentation will focus on a new approach that simplifies encryption and decryption by using a sophisticated variable content private key that can be changed quickly. The sender and the recipient are both need to have the secret color picture that is used to generate the private key. You may adjust the size of the chosen picture key so it fits the secret message exactly. Having the sender and receiver agree on a block size is a good way to increase security while sending and receiving text messages. The sender and receiver will agree on a number of bits before merging all of the bytes in a block into one vector. This vector will then be rotated to the left by that number of bits. In order to verify the benefits and accomplishments of the suggested technique, it will be put into action using a variety of color pictures and text messages, and the results will be compared to other current ways.

Keeping unwanted parties, such as abusers, invaders, or data hackers, out of text messages of varied lengths is the primary goal of this study. While making it difficult for unauthorized persons to contaminate the communications, the suggested solution streamlines the data security procedure using an innovative approach.

The use of a private key for complicated variable content is an important part of the approach. Improving system security, this private key may be changed quickly without affecting encryption and decryption processes. Both the transmitter and the recipient are needed to preserve a secret color picture that is used to produce the private key. An image key that is proportional to the secret message's length can be obtained by scaling the chosen image key.

Separating the text communication into blocks of a certain size adds another layer of protection. The method is designed to be flexible, enabling the sender and recipient to select the size of the blocks. Each block contains a vector that is comprised of individual bytes. Next, the vector is rotated to the left, with the amount of bits used

for the rotation likewise decided by the sender and receiver working together.

We will use a variety of color pictures and text messages to test the efficacy of the suggested strategy. In order to prove the merits of the suggested strategy, we shall compare the outcomes of its execution to those of other approaches.

The overarching goal of this method is to provide a simple but strong means of safeguarding text messages, reducing the likelihood of their disclosure and maximizing their secrecy.

3.2. Purpose of the Review. Protecting text messages, particularly those with sensitive or secret content, from intruders, data hackers, and illegal access is the main goal of this study. Data security may be made easier using the suggested strategy, which also makes it harder for attackers to compromise communications.

Using a complicated variable content private key is an important part of the strategy since it increases security. Changes to this private key won't affect the encryption or decryption processes that use it. A secret color picture is used to produce this private key. An picture like this may only be sent and received if both parties have it and have saved it. Finding a key length that matches the secret message is as simple as resizing the chosen picture key.

Partitioning the text message into chunks of a certain size further increases security. The sender and the recipient work together to decide on the block size, which gives them some leeway. The bytes are stacked into a single vector inside each block and then rotated to the left. Another thing that the transmitter and receiver decide is how many bits to rotate.

We will employ a variety of color pictures and text messages to test the efficacy of the suggested strategy. In order to demonstrate the merits of the proposed methodology, we shall compare the outcomes and results of this implementation to those of current methodologies.

The overarching goals of this study are to provide a strong mechanism for protecting sensitive information, make text message security easier, and increase security. The suggested method provides a workable approach to picture encryption, guaranteeing security, integrity, and resistance to possible dangers in the modern digital environment.

Here are the goals of this project:

(1) Provide a new way to safeguard text messages that is easier to use

(2) Make it more difficult for hackers to compromise communications by enhancing the security of encryption and decryption operations.

Thirdly, the encryption and decryption processes should be able to withstand changes to the private key's complicated variable content.

(4) The sender and the recipient must have the secret color picture in order to generate the private key.

(5) Make sure the secret message's length is compatible by resizing the chosen picture key.

(6) The size of each block in the text message should be decided by both the sender and the recipient.

(7) Merge all of the bytes in each block into one vector, then rotate it to the left by a mutually agreed upon amount of bits.

(8) Use a variety of color graphics and text messages to implement the suggested strategy.

(9) Show the benefits and accomplishments of the suggested approach in terms of efficiency and security by comparing its outcomes with those of current methods.

All of these goals are working toward the same goal: to make it easier and safer to safeguard text messages, make sure they are secret, and reduce the likelihood of illegal access.

3.3. Strength of Research Security. The suggested method's security strength may be further justified by looking at three crucial aspects:

One such test is the chi-square test, which looks for signs that the encrypted data follows a normal distribution. If the encryption algorithm generates results that are statistically indistinguishable from random data, then the predicted distribution may be used to compare with the observed distribution. A more robust encryption technique is indicated by a higher chi-square score.

(2) Avalanche effect: This effect determines how much a change to a single bit in the input affects the obtained ciphertext. A high avalanche effect is seen when even a little modification to the plaintext causes substantial changes to the cipher-text. It has

This attribute is very desired because it prevents attackers from deducing any information about the original data by ensuring that even slight modifications to the input lead to large and surprising changes in the output.

Thirdly, cryptanalysis entails testing the suggested approach with several types of attacks, such algebraic assaults, linear cryptanalysis, or differential cryptanalysis. These techniques evaluate the encryption algorithm's susceptibility to common attack vectors. The security strength of the algorithm may be determined by examining how well it withstands different types of assaults. It should be computationally impossible for attackers to crack an effective encryption method, so the algorithm should be resistant to these attacks.

(4) Analytical statistics: you may use statistical measurements to check

whether the encrypted output is independent, nonlinear, and random. One way to evaluate an encryption algorithm's performance is to look at its entropy, correlation coefficient, and randomness tests. A more robust encryption scheme is one with less correlation and more randomness.

These evaluations and studies will help to further justify the suggested method's security strength. Making ensuring the encrypted output is independent, nonlinear, and unpredictable is essential, as is testing the algorithm's robustness against different attack tactics. All the information about the proposed method's security features and how well it protects sensitive data can be found in these assessments.

4. Data Cryptography Method

There needs to be strong security for many of these messages, especially those that are personal or sensitive, since the use of social media has led to a dramatic increase in the amount of text messages sent and received between different parties [27]. It is critical to make sure that no one other than the intended recipient may see these communications. Using data cryptography methods is one of the most important ways to protect both short message service (SMS) and long text messages.

Encryption and decryption are the two main steps in data cryptography [27]. During encryption, a private key and a set of operations are used to change the original data into something that cannot be read or understood. When it comes time to decrypt, the encrypted data is returned to its original state by using the same private key and a different set of operations. Decryption is the process of retrieving the original material after encryption has obfuscated it. Only the sender and the recipient know the private key (PK) that is used in this cryptographic procedure, as shown in Figure 1.

The chosen method of data cryptography must adhere to the following criteria:

(1) The encryption phase should result in a high degree of data distortion, which can be quantified using quality parameters. In this study, we will employ the mean square error (MSE) as depicted in (1), peak signal-to-noise ratio (PSNR) as depicted in (2), and correlation coefficient (CC) between the original and encrypted-decrypted data.

(2) During encryption, the MSE value should be notably high, while the PSNR value should be correspond- ingly low and the CC value should significantly deviate from 1.

(3) In the decryption phase, the MSE value should ap- proach zero, indicating minimal distortion, while the PSNR value should approach infinity, indicating high-fidelity reconstruction. Additionally, the CC value should approach 1, signifying strong correla- tion between the original and decrypted data.

The selected cryptography method must fulfill the pre- requisites of effective cryptography, achieving the following objectives: optimization of quality parameters throughout encryption and decryption phases, minimization of encryption and decryption time to maximize throughput (bytes processed per second), and ensuring flexibility and ease of imple- mentation with provisions for easy acceleration if necessary. The confidential data utilized to generate the secret key must be intricate and resistant to deciphering or hacking [28].

In our research, we employ a confidential color image as the image key to generate the requisite private key for en- cryption and decryption. This choice is substantiated by several reasons:

(1) Digital color images are represented as 3D matrices, comprising individual 2D matrices for each color channel (red, green, and blue) and streamlining color image manipulation

(2) Each pixel value of the color image corresponds to an ASCII value of the message, falling within the range of 0 to 255

(3) Digital color images are readily accessible from di- verse sources at no cost

(4) The ability to work with each color matrix in- dependently facilitates various operations, notably private key generation

(5) Ease of performing operations on color matrices and resizing digital images to obtain matrices of desired dimensions (Figures 2, 3, 4, 5)

(6) The flexibility to replace the image used as the key without altering the cryptographic method, con- tingent upon agreement between sender and recipient

Utilizing a digital color image as the image key in the proposed method offers several advantages:

(1) The secrecy of the color digital image used as the key ensures its anonymity, rendering it unidentifiable

(2) The flexibility to utilize any of the colors within the image for generating the private key

(3) The capability to employ the image for generating private keys of varying sizes

(4) The ease of replacing the image with another without disrupting the method employed

5. Approach

Data Encryption Standard (DES) and its derivatives, including Advanced Encryption Standard (AES), Blowfish (BF), and many more, serve as the basis for a wide variety of secret data cryptography methods. The factors that govern the operation of these conventional approaches, as shown in Table 1 [29-31], include the number of rounds and key length.

Nevertheless, there are inherent limits to conventional encryption methods:

1. There is no way to change the key length for each technique, therefore it's not very flexible.

efficiency as well as output

The cryo-extraction procedure takes more time due to the increased round needs.

(3) The utilization of an S-box is compulsory for many approaches, which adds computational cost and memory demands.

Traditional encryption algorithms, such as Data Encryption Standard (DES), Triple DES (DES3), Advanced Encryption Standard (AES), and Blowfish, are summarized in Table 1. Although these approaches have their advantages and disadvantages, they are widely

employed for data security in a variety of applications.

One important aspect of any encryption technique is the length of the private key, which is measured in bits. While different methods provide different degrees of cryptographic strength, the length remains constant across all of them.

(2) Block size (in bits): The size of the data blocks handled during encryption and decryption is indicated by block size. The block size is constant across all methods, much as the PK length.

(3) Capacity to manage images: depicts the degree of difficulty in managing picture data using the corresponding encryption technology.

(4) Encryption quality: It explains how well each technique encrypts data, usually measured using metrics like peak signal-to-noise ratio (PSNR) and mean square error (MSE).

(5) The quality of decryption: It shows how well the decrypted data is, and it's usually assessed in terms of MSE and PSNR; in a perfect world, there would be no MSE and there would be no PSNR.

Output:

(1) Decrypted message Process:

(1) Initialization: As with encryption, start by collecting all necessary inputs.

(2) Matrix adjustment: Resize the color matrix to cor- respond with the encrypted message's length.

(3) Reversal of XOR: Apply the XOR operation between the encrypted message and the PK. This step retrieves a version of the message that was originally rotated.

(4) Block reversion:

6. Experimental Validation

Utilizing the computing capabilities of a 2.4 MHz CPU and an Intel i5 processor with 8 GB of RAM, the suggested approach was executed using MATLAB. Using a wide variety of pictures and messages of varying durations throughout deployment allowed us to comprehensively assess its efficacy across numerous circumstances. The pictures used in this procedure, carefully chosen to depict a range of features and intricacies, are shown graphically in Figure 11. Table 2 provides important information about these photos, such as their size, quality, and color depth, which complements this visual portrayal. The experimental design may be better understood with the help of this extensive dataset, which allows for a more in-depth evaluation of the effectiveness and practicality of the suggested strategy. The method's durability and dependability over a wide range of use situations are ensured by this rigorous methodology, thus enhancing its applicability and adaptability.

Figure 12 presents strong visual proof that the suggested technique outperforms conventional data encryption methods when it comes to encrypting brief messages.

Image 2 was used as an image key to choose long messages of varying lengths, and these messages were also used to implement the traditional techniques of data cryptography. The experimental outcomes for the lengthy messages are shown in Table 5.

The following details about the outcomes of the implementation for lengthy messages may be retrieved from Table 5:

(1) Encryption time and message length: The table gives information on the time it takes to encrypt a message in seconds for different message lengths in ki- lobytes (K byte). Time to decrypt using the suggested approach and industry standard methods like DES, 3DES, AES, and Blowfish (BF) are both documented.

Second, the suggested approach is efficient; it shows reduced encryption times compared to conventional methods for all message lengths. As an example, the proposed approach achieves an encryption time of 4.277896 seconds for a 30-kilobyte message, whereas the traditional methods take between 194.6700 and 1421.5 seconds.

(3) Method comparison: The suggested method's impressive efficiency in processing lengthy messages is shown by the substantial time savings it gives when compared to typical techniques of encryption.

(4) The effect of message length: both the suggested and conventional approaches experience an increase in encryption time with increasing message length. The suggested approach, on the other hand, routinely beats the state-of-the-art approaches regardless of the message length, proving that it can effectively manage massive data sets.

five, factors to consider while applying in the real world: Data transfer via networks or storage in cloud settings are two examples of applications that rely on the timely and safe encryption of large messages. The suggested solution is well-suited for these tasks since it achieves reduced encryption times.

Table 5 sheds light on the suggested method's efficiency and efficacy in encrypting large messages in comparison to traditional data encryption techniques.

Table 5 shows that the suggested solution outperforms the state-of-the-art data cryptography methods in terms of efficiency. The suggested approach significantly reduces encryption time compared to common methods like DES, 3DES, AES, and Blowfish (BF) across different message lengths, as shown in the table. The method's efficacy in safely processing massive amounts of data is shown by the very noticeable efficiency boost for lengthy communications. Moreover, they are graphically reinforced in Figure 13.

result, showing that the suggested approach is more efficient in real-world cryptographic applications than typical methods, and that

the difference in encryption times is clear.

Experiment results show that the proposed cryptography approach is competitive with, and often outperforms, more conventional algorithms. For secure communication applications that need efficient and reliable encryption, it provides a strong solution for data security while also offering fast throughput and decreased processing times.

REFERENCES

[1] "Rotational cryptographic technique (RCT)" by D. Guha, R. Chakraborty, and J. K. Mandal, in Learning and Analytics in Intelligent Systems, pp. 150-156, Cham, Germany, March 2020.
on the 2021 issue of the IEEE Transactions on Information Forensics and Security, the authors L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong discuss "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs." The article is located on pages 1681-1695 and was published in volume 16.

International Journal for the History of Engineering and Technology, vol. 1, no. 2, 2022, "The application of encryption and decryption to the delivery of text messages using the Rc4 algorithm (rivest code 4) utilizes the lsb (least significant bit) algorithm as an insertion into the image" [3] (Al Boy In, A. Fauzi, and H. Sembiring).

[4] "Conditional privacy-preserving authentication scheme without using point multiplication operations based on el-liptic curve cryptography (ECC)" (IEEE Access, vol. 8, J. S. Alshudukhi, B. A. Mohammed, and Z. G. Al-Mekhlafi, 2008). volumes 22, 20, 32, and 40, 2020.

In 2020, F. Ramadhani, U. Ramadhani, and L. Basit published an article in the Journal of Computer Science, Information Technology and Telecommunication Engineering titled "Combination of hybrid cryptography in one time Pad (OTP) algorithm and keyed-hash message authentication code (HMAC) in securing the WhatsApp communication application." The article can be found on pages 31–36.

[6] In the 2020 issue of the Al-Qadisiyah Journal Of Pure Science, the author H. Najeeb discusses the use of cryptography and steganography to conceal a voice communication.

"Cryptography as information control" (S. M. West, 2022, pp. 351-375) was published in the Social Studies of Science.

According to a study published in the International Journal of Advanced Research in Science, Communication and Technology in 2022, P. Wani, A. Nanaware, S. Shirode, A. Suram, and A. Jadhav discussed the use of multi-image steganography for secret communication in a military context.

The article "Proficient and safe token with secret and public keys sharing algorithm for preventing cryptographic key leakage in wireless sensor network" was published in the International Journal of Engineering Research in Electronics and Communication Engineering in 2022 and was written by R. Nesamalar and K. Ravikumar.

Article cited as "An efficient least significant bit image steganography with secret writing and compression tech-niques" by J. C. T. Arroyo in the 2020 issue of the International Journal of Advanced Trends in Computer Science and Engineering, volume 9, issue 3, pages 3280–3286.

An article titled "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message" was published in the Journal of Physics: Conference Series in 2022 and was written by R. Hammad, K. Abdul Latif, A. Zuli Amrullah, and others.

"Secret messages in enigmatic playful texts," Archives in Biomedical Engineering and Biotechnology, volume 4, issue 2, 2020, written by R. Gobato.

"Enhancing the security of the diffie-hellman key exchange protocol using RSA cryptography," published in the Journal of Physics: Conference Series in 2022, was written by C. Gupta and N. V. S. Reddy. With the help of A. Al-Hasanat, K. Matrouk, H. Alasha'ary, and

In the World Applied Sciences Journal, Z. Al-Qadi Al-Shalabi published an article titled "Speech fingerprint to identify isolated word person" in volume 31, issue 10, 2014, pp. 1767-1771.

[15] "Image hiding using LSB insertion method with improved security and quality," published in the International Journal of Science and Research in 2014, volume 3, issue 9, pages 2281-2284. Mr. Jose is the author of this work.

16 "An improved LSB based Steganography with enhanced Security and Embedding/Extraction," presented by M. Juneja and P. S. Sandhu at the 2013 3rd International Conference on Intelligent Computational Systems in Hong Kong, China.
"Using wave equation to extract digital signal features," published in Engineering, Technology and Applied Science Research, volume 8, issue 4, pages 3153-3156 in 2018, was written by A. Al-Rawashdeh and Z. Al-Qadi.