A Star Number-Based Approach for Secure Image Encryption and Decryption

M.Suruthika1, P.Geetha1,a)

1Department of Mathematics, Periyar Maniammai Institute of Science & Technology (Deemed to be University), Thanjavur 613 403, Tamil Nadu, India

Corresponding Author: a)[geethamaths@pmu.edu](mailto:geethamaths@pmu.edu)

**Abstract:** This paper presents a novel image encryption and decryption technique based on the Star Number sequence combined with the bitwise XOR operation for both grayscale and color images. The proposed method generates a deterministic yet non-linear key matrix from the mathematical properties of Star Numbers, ensuring strong confusion and resistance to brute-force and statistical attacks. For grayscale images, encryption is done to a single intensity channel, and in the case of color images, the same key matrix is utilized independently to the Red, Green, and Blue channels. Histogram analysis shows that the encrypted images possess an almost uniform distribution of pixel intensity, which efficiently conceals the statistical characteristics of original images. Reversibility of the XOR operation guarantees lossless decryption, further confirmed by pixel-by-pixel verification of original and recovered images. Comparative study shows that grayscale encryption is computationally more cost-effective but color encryption offers greater security owing to multi-channel scrambling. The scheme is effective, secure, and suitable for real-time medical imaging, defense communication, and secure digital storage applications.

**Keywords:** Image Encryption, Star Number Sequence, XOR Operation, Grayscale and Color Images, Histogram Analysis.

# ****Introduction****

**The increasing rate of digital communication has increased the necessity for secure image data transmission over public and private networks [1]. Images may contain sensitive information in fields like telemedicine, surveillance applications, and confidential documents, where unauthorized use can produce undesirable outcomes. Conventional cryptographic primitives such as AES and DES, while secure for text data, can be computationally inefficient on image scales because of the extremely high pixel redundancy and intense spatial correlation that are characteristics of image data. To counter these problems, specially designed image-based encryption schemes have been developed, which concentrate on destroying pixel correlation along with ensuring computational efficiency. One such appealing method is the use of mathematical sequences to create cryptographic keys. We introduce in this work an image encryption scheme grounded on the Star Number sequence, a family of figurate numbers known for their deterministic but intricate form. An array of pixel-wise key is produced by applying the sequence to produce a pixel-wise key matrix, with which the image data are combined through the bitwise XOR operation.**

The proposed method is implemented for both grayscale and color images. In the grayscale case, encryption operates on a single intensity channel, ensuring rapid computation [2]. In the color case, encryption is applied separately to each RGB channel, increasing statistical randomness and security strength. Experimental results, including histogram analysis and performance verification, confirm the effectiveness and robustness of the approach.

# ****Literature Review****

The last few years have witnessed the development of a number of image encryption techniques, both of which fall into the general categories of spatial-domain and transform-domain techniques[3]. Spatial-domain techniques, such as pixel scrambling and bitwise logical operations, offer good computational speed and are suitable for real-time applications. Transform-domain techniques, such as using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), offer better frequency-domain security but at the cost of higher computational complexity. Chaotic maps have found extensive applications in image encryption because of their pseudo-random and sensitivity to initial conditions. Logistic, Henon, and Lorenz maps have been utilized to produce key streams for the permutation and diffusion stages. Although these techniques are good sources of randomness, they tend to have floating-point operations, which decrease computational efficiency and make it difficult to implement in hardware[4].

Number theory-based methods have also gained attention, using mathematical sequences like Fibonacci numbers, Lucas numbers, and prime sequence numbers for key generation [5].These types of methods provide deterministic key reproduction with low storage costs. Nevertheless, predictability for some sequences makes them susceptible to attacks unless constructed suitably with encryption processes. The Star Number sequence, while not as advanced in cryptography, does have one specific advantage: generation is deterministic but produces non-linear growth patterns immune to instant prediction [6]. When the sequence is processed with the XOR operation, it generates a good and secure encryption scheme which can encrypt color and grayscale images. In contrast to previous schemes, the new scheme provides a balance between security against brute-force and statistical attacks, computational efficiency, and ease of implementation.

## Gray Image Processing

## Image Acquisition and Preprocessing

In the first phase of the proposed encryption algorithm, the original image is loaded from the local storage. Since the encryption algorithm can encrypt grayscale images only, a colored image (RGB mode) is first converted into its grayscale variant[7]. Such a transformation reduces data representation by mapping three color channels (red, green, and blue) into a single intensity channel, thus reducing computational complexity without losing essential visual details. The image is then resized to a common resolution of 256 × 256 pixels upon conversion. This resizing ensures that all experimental tests are performed on images of uniform size, allowing fair comparison of results and ensuring uniformity in key generation and encryption processes. The resizing procedure also supports compatibility with fixed-size key matrix obtained from the Star Number sequence.

In addition, the pixel values are converted to 8-bit unsigned integer (uint8) format explicitly, which limits the intensity level range between 0-255. This is required because the XOR-based encryption operation is best performed on 8-bit quantities so that the pixel values as well as key values fall within a uniform range[8]. These preprocessing operations altogether guarantee that the input image is in a format that is completely compatible with the following key generation and encryption operations, hence facilitating effective and accurate encryption and decryption(*Figure 1)*.

## Star Number Sequence-Based Key Generation

The security of the proposed image encryption method relies heavily on the generation of a robust and unpredictable key. In this work, the key is derived from the Star Number sequence, a special class of figurate numbers with a distinct mathematical pattern. The sequence is defined by the formula [9]:

……(1)

Where represents the sequence index, starting from up to , the total number of pixels in the image. This mathematical formulation generates a deterministic yet non-linear progression of numbers, which can serve as an effective basis for key generation in cryptographic applications. Once the sequence is generated for all N pixels, each value is taken modulo 256 to ensure it falls within the 8-bit integer range (0-255). This mapping is crucial to maintain compatibility with the pixel intensity values of the grayscale image. The resulting key stream is then reshaped into a key matrix that has the same dimensions as the image[10]. This matrix is used to perform pixel-wise encryption using the XOR operation, ensuring that each pixel has a unique key value. The use of the Star Number sequence adds mathematical complexity and enhances resistance to brute-force and statistical attacks.

## Encryption Process

The encryption process in the proposed method utilizes the bitwise XOR (exclusive OR) operation, which is widely recognized for its simplicity, reversibility, and effectiveness in cryptographic applications [11]. Once the key matrix is generated from the Star Number sequence, each pixel of the preprocessed grayscale image is encrypted individually by performing an XOR operation with the corresponding pixel value from the key matrix. Mathematically, the encryption process can be expressed as:

……(2)

Where is the intensity value of the original image at position is the corresponding key value from the key matrix, and is the resulting encrypted pixel value. This operation significantly alters the pixel intensity distribution, producing an image that appears as random noise and is visually unrecognizable. Since the XOR operation is highly sensitive to the key values, even a small change in the key sequence produces a completely different encrypted output(*Figure 1)*. Furthermore, because XOR is a symmetric operation, it guarantees lossless reversibility, enabling accurate decryption when the same key is used(*Table 1)*. This step ensures strong confusion of pixel values, enhancing the overall security of the encryption scheme.

## Decryption Process

The decryption stage in the proposed scheme is a direct reversal of the encryption process, utilizing the same bitwise XOR operation. Due to the symmetric nature of XOR, applying the identical key used for encryption to the cipher text restores the original pixel values without any loss of information[12]. This property ensures that the process is both reversible and computationally efficient. Mathematically, the decryption can be expressed as:

……(3)

Where represents the encrypted pixel value, is the corresponding key value from the Star Number sequence, and is the recovered pixel value. Since , performing XOR twice with the same key effectively cancels out the key influence and retrieves the original data[13]. The process guarantees lossless recovery, meaning the decrypted image is identical to the original image at the pixel level (*Figure 1)*. This reversibility is crucial in applications where exact data restoration is required, such as medical imaging or secure government communications. The correctness of decryption is verified by comparing the decrypted image with the original, ensuring that no distortion or information loss has occurred during encryption and decryption.

### Pseudo code

BEGIN

1. Load Image

Read input image from file

If image is RGB, convert it to grayscale

Resize image to 256 × 256 pixels

Convert pixel values to 8-bit integers

2. Generate Key Matrix (Star Number Sequence)

rows ← number of rows in image

cols ← columns in picture

N ← rows × cols

For n from 1 to N do

star\_num[n] ← 6 × n × (n − 1) + 1

key\_stream[n] ← star\_num[n] mod 256

End For

Redimension key\_stream to key\_matrix of (rows, cols) size

3. Encryption (XOR Operation)

encrypted\_img ← bitwise XOR between img and key\_matrix

4. Decryption (XOR Again)

decrypted\_img ← bitwise XOR between encrypted\_img and key\_matrix

5. Display Images and Histograms

Display original, encrypted, and decrypted images

Plot histograms for original, encrypted, and decrypted images

6. Verification

If decrypted\_img equals img then

Print "Decryption successful!"

Else

Print "Decryption failed!"

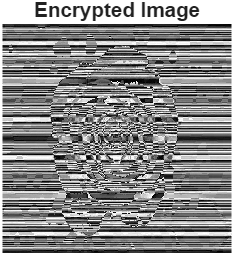
End If

END

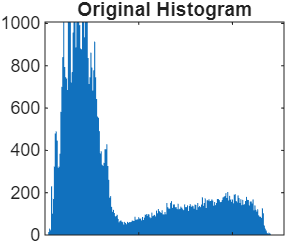
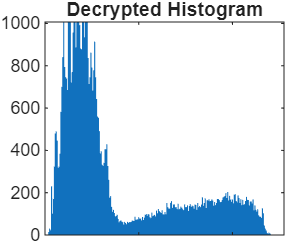
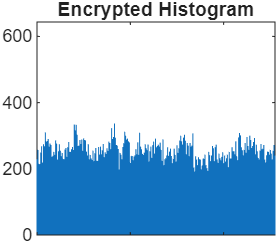
## ****Histogram Analysis****

**Histogram analysis is a critical step in quantifying the efficiency of an image encryption scheme since it statistically and graphically represents the intensity distribution of pixels in an image[14]. In the proposed method, histograms are plotted for the original image, encrypted image, and decrypted image to verify if there has been a change in intensity patterns before and after encryption. The histogram of the original image tends to show a non-uniform shape with peaks indicating the presence of redundant intensity values, which can be utilized for statistical attacks. The histogram of the encrypted image should, however, show a near-uniform shape across the 0-255 range of intensities. This homogeneity indicates that pixel values are homogeneously distributed, actually concealing original image structure and reducing the likelihood of successful statistical analysis[15].**

**The decrypted image histogram must exactly replicate the original image histogram, indicating that the encryption process is reversible and lossless. This replication ensures that the suggested algorithm does not cause any distortion or data loss during the encryption and decryption processes(**Table 1)**.**

1. (B) (C)

(D) (E) (F)

Figure 1: (A)-(F) Original, Encrypted, and Decrypted Grayscale Images with Corresponding Histograms

## Performance Verification

Performance verification is an essential phase to prove that the suggested encryption-decryption mechanism works well and supports lossless retrieval of data. At this stage, the original image and decrypted image are compared pixel-wise. The comparison is carried out by a logical equality check by comparing each respective pixel value of the original and decrypted images. If all the pixel values are identical, it confirms that decryption has revived the original image effectively with no change or loss of information.

In the method presented here, verification is based on the reversibility of the XOR operation. Because repeating the same key twice (for encryption and decryption) annuls its effect, the reconstructed image is ensured to be identical to the original image as long as the proper key is applied. A successful verification not only ensures the correctness of the algorithm but also certifies its applicability for applications needing perfect reconstruction, such as secure image transmission for military, medical, or confidential government communications. Any mis-match at this stage would point towards a fault in key generation, encryption, or decryption steps, and thus this verification step forms a critical part of the overall security evaluation.

## RGB Image Processing

### **Image Acquisition and Preprocessing**

**At the first step in the suggested color image encryption scheme, the target image is obtained from the local storage system. The image to be encrypted is processed in its original RGB color space, which consists of three separate channels: Red, Green, and Blue[16]. Unlike grayscale processing, where the image is compounded into one intensity channel, the RGB notation maintains the full color information, thus making the encryption more difficult to pass through and thus more secure. To ensure consistency in testing the encryption performance and for compatibility with the key generation process, the picture is resized to the standard resolution of 256 × 256 pixels. This constant size eases implementation through the ability to maintain the overall number of pixels per channel the same across experiments, further enabling direct mapping of the resulting key matrix to the image size without further adaptation.**

**After being resized, the pixel data is also converted explicitly into the 8-bit unsigned integer (uint8) format.This is accomplished in order to have the pixel intensity values between the 0-255 range, as appropriate for the operation range of the bitwise XOR encryption process [16]. This step is required in order to avoid computational inconsistencies and make the key value compatible with the Star Number sequence. Lastly, the image size-the number of colour channels, rows, and columns-is derived. These are crucial for subsequent processing, like constructing the key stream and encrypting each channel individually. Upon normalising the input data, the preprocessing operation retains valuable image data and prepares the image for secure and efficient encryption and decryption procedures in subsequent stages.**

## Star Number Sequence-Based Key Generation

The security of the proposed encryption scheme relies on the generation of a strong and mathematically structured key. In this work, the key is derived from the Star Number sequence, a class of figurate numbers characterized by their geometric and arithmetic properties. The sequence is generated using the formula [14]:

……(4.2.1)

Where denotes the sequence index, ranging from to , where is the total number of pixels in a single color channel of the image. This formula produces a deterministic, non-linear progression of numbers, which increases rapidly with n and provides a complex key pattern that is difficult to predict. Once the Star Number sequence is generated for all pixels, the values are mapped into the 8-bit range (0–255) using the modulo operation:

……(4.2.2)

This step ensures pixel intensity range compatibility with the RGB image and facilitates effortless integration into the XOR encryption process. The resulting values constitute a key stream, which is then reshaped into a key matrix corresponding to the spatial size of the image (row ×columns). The identical key matrix is independently used for each of the RGB channels in encryption. This method adds pixel-wise variation in each channel to provide higher resistance to brute-force, statistical, and differential attacks[18]. In addition, as the Star Number sequence is deterministic, the key can be exactly replicated when decrypting without having to store or transfer a huge volume of key data to maintain both security and efficiency in encryption.

## Encryption Process

The encryption step of the suggested approach utilizes the bitwise XOR (exclusive OR) operation, which is a common and effective method in cryptographic systems because it is simple, reversible, and has strong confusion characteristics. In this scheme, encryption is performed separately on each color channel (Red, Green, and Blue) of the RGB image to guarantee that all channels are safely scrambled[19]. For every channel, the pixel values of the original image are being mixed with the respective values of the Star Number–based key matrix using XOR operation:

……(4.3.1)

Where is the pixel value at position in channel , is the key value at the same position, and is the resulting encrypted pixel value. This operation alters the binary representation of each pixel based on the corresponding key value, producing an encrypted image in which pixel intensities are significantly different from the original(*Figure 2)*. The XOR operation ensures high sensitivity to key values. Even a single-bit change in the key will result in a completely different encrypted output, making the method resistant to brute-force and differential attacks[20]. Additionally, since XOR is a symmetric operation, the same process can be reversed during decryption to recover the original image without any loss of information. By applying this process to all three channels independently, the encryption not only hides the spatial distribution of pixel values but also effectively conceals the color composition of the original image, resulting in a visually unrecognizable encrypted output with high randomness in each channel.

## Decryption Process

The decryption stage in the proposed color image encryption scheme is a direct reversal of the encryption process, utilizing the same bitwise XOR (exclusive OR) operation. Since XOR is a symmetric and reversible operation, applying the identical key used during encryption to the encrypted image restores the original pixel values without any loss of information. This property is mathematically expressed as[21]:

……(4.4.1)

Where represents the encrypted pixel value at position in channel, is the key value from the Star Number sequence, and is the recovered pixel value. Due to the property, the application of the same key twice cancels out its effect, allowing perfect reconstruction of the original image. Decryption is performed separately for each RGB channel, ensuring that all color information is accurately restored(*Figure 2)*. Since the key matrix is generated deterministically from the Star Number sequence, it does not need to be stored or transmitted; the receiver can reproduce it if the initial parameters are known. The effectiveness of this stage is confirmed through pixel-by-pixel comparison between the decrypted and original images. If all pixel values match exactly, the decryption is deemed successful. This guarantees lossless recovery, which is essential for applications such as medical imaging, defense communications, and secure archival storage, where even a single bit of data loss is unacceptable. Thus, the decryption process ensures both data integrity and security while maintaining computational efficiency[22].

BEGIN

1. Load and Preprocess Color Image

Read the input image from file

Resize image to 256 × 256 pixels

Convert pixel values to 8-bit integers

rows ← number of rows

cols ← number of columns

ch ← number of channels (3 for RGB)

N ← rows × cols // pixels per channel

2. Generate Star Number Key Matrix

For n from 1 to N do

star\_num[n] ← 6 × n × (n − 1) + 1

key\_stream[n] ← star\_num[n] mod 256

End For

Reshape key\_stream into key\_matrix of size (rows, cols)

3. Encryption (Channel-wise XOR)

For c from 1 to ch do

encrypted\_channel[c] ← img\_channel[c] XOR key\_matrix

End For

Combine encrypted channels into encrypted\_img

4. Decryption (Channel-wise XOR)

For c from 1 to ch do

decrypted\_channel[c] ← encrypted\_channel[c] XOR key\_matrix

End For

Combine decrypted channels into decrypted\_img

5. Display Results

Show original, encrypted, and decrypted images

Plot RGB histograms for original, encrypted, and decrypted images

6. Verification

If decrypted\_img equals img then

Print "Decryption successful!"

Else

Print "Decryption failed!"

End If

END

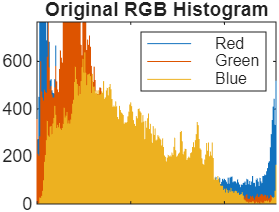
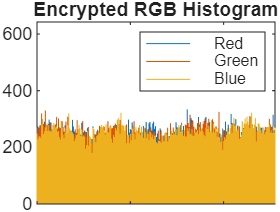
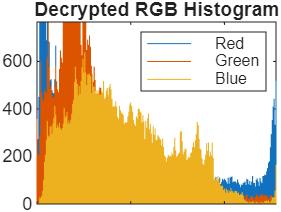
## ****Histogram Analysis for Color Images****

Histogram analysis is employed to compare the statistical characteristics of original, encrypted, and decrypted color images within each RGB channel. The histogram is the pixel intensity frequency distribution (0-255) of a channel[23]. In an original image, the histogram of each channel normally displays distinct peaks and skewed distributions, indicating the inherent intensity changes and color patterns of the image. Such regular structure can be exploited in statistical attacks if it is not well hidden.

Conversely, the histograms of the three channels of the encrypted image have a very uniform distribution. This uniformity suggests that intensities of pixels are homogeneously distributed over the entire range, and thereby it is very challenging for the attackers to derive useful patterns or deduce original pixel values[24]. Lastly, the decrypted image histograms exactly match the original image histograms(*Figure 2)*, ensuring that the encryption-decryption algorithm is lossless and maintains the original image information without any form of distortion. The above analysis ensures both the security robustness and correctness of the introduced color image encryption technique.

(A) (B) (C)

(D) (E) (F)

Figure 2: (A)-(F) Original, Encrypted, and Decrypted Color Images with RGB Channel Histograms

## ****Performance Verification****

**Performance verification ensures that the proposed encryption–decryption process operates correctly and restores the original image without any loss of information. In this step, the decrypted image is compared with the original image on a pixel-by-pixel basis. If every corresponding pixel value matches exactly, the process confirms lossless recovery. This verification is possible due to the reversible property of the XOR operation, where applying the same key twice () eliminates the encryption effect and retrieves the original pixel values[25]. The key matrix, generated from the Star Number sequence, is deterministic, ensuring that the same key can be reproduced at the decryption stage without direct transmission. A successful verification not only confirms the accuracy of the algorithm but also its robustness for applications where data integrity is critical, such as medical imaging, defense communications, and secures data storage. Any mismatch in the comparison would indicate errors in key generation, encryption, or decryption, making this step an essential validation stage for the overall security and reliability of the system.**

## Comparative Analysis of Grayscale and Color Image Encryption using Star Numbers

The fundamental difference between grayscale and color image encryption lies in the data representation of the image. A grayscale image contains only intensity information, with each pixel represented by a single 8-bit value (0-255) corresponding to brightness. This makes processing simpler because the encryption algorithm operates on one channel only, applying the Star Number-based key matrix directly to the pixel matrix using the bitwise XOR operation. In contrast, a color image is composed of three independent channel-Red, Green, and Blue-each storing its own 8-bit intensity value for every pixel. Thus, encryption must be applied separately to each channel(*Table 1)*. In the proposed method, the same Star Number-based key matrix is reused for all three channels, ensuring that every pixel in each channel is transformed individually. This increases computational workload compared to the grayscale case but results in higher security strength because the scrambling effect is spread across all channels, making the encrypted image visually more chaotic(*Table 1)*.

Table 1: Comparative Analysis of Grayscale and Color Image Encryption Using Star Number Sequence

| **Features** | **Grayscale Image Encryption** | **Color Image Encryption** |
| --- | --- | --- |
| **Image Channels** | Single channel (intensity only). | Three channels (Red, Green, Blue) processed independently. |
| **Preprocessing** | If RGB, convert to grayscale; resize to 256×256; store as uint8. | Load RGB image directly; resize to 256×256; store as uint8. |
| **Pixel Value Range** | 0–255 (8-bit) intensity values. | 0–255 per channel, 8-bit values for  R, G, B. |
| **Key Generation** | Star Number sequence of length  N = rows × cols. | Star Number sequence of length  N = rows × cols (per channel). |
| **Key Matrix Application** | Applied directly to single grayscale channel. | Same key matrix applied to each of the three channels separately. |
| **Encryption Formula** |  | per channel . |
| **Decryption Formula** |  | per channel . |
| **Histogram Analysis** | Single histogram before/after encryption. | Separate histograms for R, G, and B channels. |
| **Security Effect** | Randomizes grayscale intensity distribution. | Randomizes pixel values in all color channels, stronger visual scrambling. |
| **Verification** | Compare decrypted grayscale image with original. | Compare decrypted RGB image with original. |
| **Computation Load** | Lower - processes only one channel. | Higher - processes three channels, but still efficient due to XOR. |

From a cryptographic point of view, the pixel-wise XOR operation gains equally in both grayscale and color situations owing to its reversibility and extreme sensitivity to key modifications. In the color situation, however, the histogram analysis needs to be carried out independently for each channel [26][27]. The encrypted RGB histograms usually turn out to be uniformly distributed, which confirms successful elimination of statistical patterns in every channel(*Table 1)*. The decision between grayscale and color encryption is application-dependent. Grayscale encryption can be used in situations when color is not important (e.g., medical imaging, documents) and provides more rapid processing with reduced memory requirements. Color encryption is mandatory for applications such as secure transmission of natural images, where the full image content must be retained at all costs, even if it consumes additional processing resources. Therefore, although the underlying encryption algorithm is the same, the data dimensionality in color images adds complexity, computational overhead, and statistical strength, giving it a better but heavier encryption scheme than grayscale processing.

# ****Conclusion****

This article suggested an effective image encryption and decryption process based on the Star Number sequence augmented with bitwise XOR operation for both grayscale and color images. The Star Number-based key matrix, derived deterministically, provides pixel-wise encryption with excellent confusion properties. For grayscale images, a single intensity channel is encrypted, allowing for very rapid computation. For colored images, the same key is uniformly applied separately to the RGB channels in order to further enhance statistical randomness and visual jumbling. Histogram analysis proved that encrypted images have almost uniform intensity histograms, successfully hiding the statistical patterns of the original images. The self-symmetry of XOR guarantees lossless recovery, verified by pixel-by-pixel comparison between recovered and original images. Comparative results show that grayscale encryption is more computationally economic and color encryption provides better statistical attack resilience by multi-channel processing. Owing to simplicity, low processing cost, and excellent security performance, the proposed method is appropriate for secure image transmission in real-time, medical imaging, and military communication.

# References

1. Naeem, E., Abdelaal, A., Eyssa, A., Alazrak, F., Ahmed, R., Hassan, E., Elashry, I., Elkorany, A., Elsharkawy, Z., Elnaby, M., Faragallah, O., Dessouky, M., Abd-Elnaby, M., Ahmed, Z., El-Rabaie, E., & El-Samie, F. (2020). Efficient signal and protocol level security for network communication. International Journal of Speech Technology, 23, 399 - 424. <https://doi.org/10.1007/s10772-019-09607-8>.
2. Olvera-Martinez, L., Cedillo-Hernandez, M., Diaz-Rodriguez, C., Faustinos-Morales, L., Cedillo-Hernández, A., & Garcia-Ugalde, F. (2025). Symmetric Grayscale Image Encryption Based on Quantum Operators with Dynamic Matrices. Mathematics. <https://doi.org/10.3390/math13060982>.
3. Sudha, T., & Gopi, B. (2014). Novel Spatial and Transform Domain Image Encryption Algorithms. IOSR journal of VLSI and Signal Processing, 4, 38-45. <https://doi.org/10.9790/4200-04223845>.
4. Rizki, M., Iman, E., Ujianto, H., & , R. (2023). Digital Image Encryption Using Logistic Map. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). <https://doi.org/10.29207/resti.v7i6.5389>.
5. K, G. (2023). APPLICATIONS OF NUMBER THEORY IN CRYPTOGRAPHY. ShodhKosh: Journal of Visual and Performing Arts. <https://doi.org/10.29121/shodhkosh.v4.i2.2023.4021>.
6. Yao, B., Wang, X., F., & Wang, H. (2021). Number-Based Strings And Degree-sequences Of Topological Cryptography. 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 5, 791-796. <https://doi.org/10.1109/IAEAC50856.2021.9391000>.
7. Olvera-Martinez, L., Cedillo-Hernandez, M., Diaz-Rodriguez, C., Faustinos-Morales, L., Cedillo-Hernández, A., & Garcia-Ugalde, F. (2025). Symmetric Grayscale Image Encryption Based on Quantum Operators with Dynamic Matrices. Mathematics. <https://doi.org/10.3390/math13060982>.
8. Jahangir, S., Shah, T., & Ismail, A. (2023). An algebraic and chaotic three-layered digital data encryption technique. Nonlinear Dynamics, 111, 20407-20423. <https://doi.org/10.1007/s11071-023-08835-7>.
9. M., V., Kunte, R., & Chandrappa, V. (2023). Encryption Using Binary Key Sequences in Chaotic Cryptosystem. International Journal of Computer Network and Information Security. <https://doi.org/10.5815/ijcnis.2023.04.05>.
10. Khudhair, Z., Khdiar, A., Abbadi, N., Mohamed, F., Saba, T., Alamri, F., & Rehman, A. (2023). Color to Grayscale Image Conversion Based on Singular Value Decomposition. IEEE Access, 11, 54629-54638. <https://doi.org/10.1109/ACCESS.2023.3279734>.
11. A, S., , S., , S., C, S., & Shetty, S. (2025). XOR CIPHER. International Journal on Science and Technology. <https://doi.org/10.71097/ijsat.v16.i1.2550>.
12. Negi, A., Saxena, D., & Suneja, K. (2020). High Level Synthesis of Chaos based Text Encryption Using Modified Hill Cipher Algorithm. 2020 IEEE 17th India Council International Conference (INDICON), 1-5. <https://doi.org/10.1109/INDICON49873.2020.9342591>.
13. K., Teng, L., Wang, X., & Meng, J. (2021). Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory. Multimedia Tools and Applications, 80, 24737 - 24757. <https://doi.org/10.1007/s11042-021-10847-7>.
14. Malik, D., & Shah, T. (2020). Color multiple image encryption scheme based on 3D-chaotic maps. Math. Comput. Simul., 178, 646-666. <https://doi.org/10.1016/j.matcom.2020.07.007>.
15. Anitha, P., & Vallinayagi, V. (2022). improved data hiding approach on color images using difference expansion algorithm. International journal of health sciences. <https://doi.org/10.53730/ijhs.v6ns1.7862>.
16. Ghadirli, H., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. Signal Process., 164, 163-185. <https://doi.org/10.1016/J.SIGPRO.2019.06.010>.
17. Xu, P., Wu, Q., Wang, W., Susilo, W., Domingo-Ferrer, J., & Jin, H. (2015). Generating Searchable Public-Key Ciphertexts With Hidden Structures for Fast Keyword Search. IEEE Transactions on Information Forensics and Security, 10, 1993-2006. <https://doi.org/10.1109/TIFS.2015.2442220>.
18. Al-Laham, M. (2015). E NCRYPTION -D ECRYPTION RGB C OLOR I MAGE U SING M ATRIX M ULTIPLICATION. . <https://doi.org/10.5121/ijcsit.2015.7508>.
19. Telem, A., Tchapga, C., De Dieu Nkapkop, J., De Dieu Nguimfack Ndongmo, J., Tsafack, N., & Boya, B. (2024). Hyperchaotic color image encryption scheme based on simultaneous color channel confusion-diffusion operations. Physica Scripta, 99. <https://doi.org/10.1088/1402-4896/ad5629>.
20. Hagras, T., Salama, D., & Youness, H. (2022). Anti-attacks encryption algorithm based on DNA computing and data encryption standard. Alexandria Engineering Journal. <https://doi.org/10.1016/j.aej.2022.05.033>.
21. Dodmane, R., Aithal, G., & Shetty, S. (2022). Construction of vector space and its application to facilitate bitwise XOR - Free operation to minimize the time complexity. J. King Saud Univ. Comput. Inf. Sci., 34, 9836-9843. <https://doi.org/10.1016/j.jksuci.2021.12.015>.
22. Wallack, S. (2008). Digital image storage.. Veterinary radiology & ultrasound : the official journal of the American College of Veterinary Radiology and the International Veterinary Radiology Association, 49 1 Suppl 1, S37-41 .
23. Tanji, K., Itoh, H., & Imiya, A. (2018). Application of Directional Statistics to Classification of Three-Channel Colour Images. , 60-69. <https://doi.org/10.3233/978-1-61499-929-4-60>.
24. Aggarwal, A., Awasthi, E., Kukreja, D., Kedia, J., & Bala, I. (2024). Modified moth flame optimization and logistic chaotic map integration for image encryption. Int. J. Syst. Assur. Eng. Manag., 16, 785-804. <https://doi.org/10.1007/s13198-024-02669-1>.
25. Guo, Y., Li, W., Wu, L., & Zhai, P. (2024). Robust optical multi-image encryption with lossless decryption Recovery Based on phase recombination and vector decomposition. iScience, 27. <https://doi.org/10.1016/j.isci.2024.110574>.
26. Wang, H., Jiang, Z., Qian, Q., & Wang, H. (2022). An efficient XOR-based visual cryptography scheme with lossless reconfigurable algorithms. International Journal of Distributed Sensor Networks, 18. <https://doi.org/10.1177/15501329221084223>.
27. Dhakal, M., & Shakya, S. (2025). Enhancing Image Data Security: DNA Cryptography and XOR-Based Feistel Encryption. Journal of Innovative Image Processing. https://doi.org/10.36548/jiip.2025.1.001.