Grenze International Journal of Engineering and Technology, January Issue

Visual Cryptography using Sigmoid and Transposition Cipher Technique

Anitha S Prasad[1], Usharani C M[2], Sneha S[3] and Keerthana B[4]
[1-4]Department of ECE, SJCE, JSSSTU, Mysore, India
Email: anith.sp@sjce.ac.in, usharani@jssstuniv.in, snehagowda0502@gmail.com, Keerthi67854@gmail.com

***Abstract*— In a world where secure image transmission is crucial—especially in areas like telemedicine, surveillance, and digital documentation—this paper presents a novel visual cryptography approach that protects image data while also enhancing its clarity. Traditional cryptographic techniques often burden systems with complex computations or degrade visual quality. To address this, the proposed work consist of a dual- layer method: first, an image is encrypted using a transposition cipher that scrambles pixel positions based on a secure, hashed key; second, a sigmoid function is applied to enhance contrast, ensuring the final image is both secure and visually sharp. This method ensures that even if unauthorized users access partial data, the image remains unreadable and visually distorted. The process involves converting images into matrix form, applying encrypted sorting operations on rows and columns, and then enhancing contrast using a sigmoid transformation that improves brightness differentiation without introducing noise. The encryption and decryption steps are carefully designed to reverse each other, maintaining the integrity of the original image. The proposed technique was implemented in MATLAB and validated through histogram analysis, which showed that the encrypted images had high randomness, while decrypted images preserved structural and contrast details. Overall, the method achieves a strong balance between image security and visual quality, making it highly suitable for real-time, resource- constrained applications.**

***Index Terms*— Visual Cryptography, Sigmoid Function, Columnar Transposition Cipher, Image Encryption, Contrast Enhancement, Secure Image Transmission.**

I. INTRODUCTION

In the era of rapidly expanding digital communication, ensuring the confidentiality, integrity, and clarity of visual data has become a critical requirement across domains such as telemedicine, surveillance, and digital documentation. With the increasing exchange of sensitive image data over open networks, conventional cryptographic methods like Rivest-Shamir Adelman(RSA) and Advanced Encryption Standard(AES), although secure, often introduce computational overhead and may degrade image quality. Visual cryptography (VC) presents a lightweight and human readable solution by splitting an image into multiple shares, such that stacking them reveals the original content. However, existing VC techniques frequently suffer from low contrast, making the decrypted image difficult to interpret. This becomes a major limitation in applications where image clarity is paramount. Traditional image encryption schemes including Least Significant Bit (LSB) substitution, Discrete Wavelet Transform (DWT) - based steganography, and Elliptic Curve Cryptography (ECC) provide varying levels of security, but often at the cost of increased computational Complexity ordegraded image contrast.

Grenze ID: 01.GIJET.12.1.24_2

Furthermore, these Methods do notinherently address the readability of the decrypted image. To tackle these challenges, our research introduces a novel technique that integrates an adaptive sigmoid function For enhancing the contrast of the encrypted image with a Columnar transposition cipher to increase the level of security. The sigmoid function, applied in the spatial domain, ensures that contrast is improved without introducing noise, while preserving the mean brightness and structure of the original image. The uniqueness of this approach lies in its two layered protection mechanism: one that boosts visual clarity through nonlinear intensity transformation, and another that scrambles the pixel positions using a symmetric key encryption scheme. This combination ensures that even if an attacker gains partial access to the shares, the image remains unintelligible. Histogram analysis is used to evaluate be effectiveness of the encryption process, the randomness of the generated shares and the quality of the reconstructed image. This evaluation ensures that the cryptographic scheme is secure and maintains acceptable visual fidelity. The goal of this paper is to demonstrate how combining contrast enhancement with lightweight cryptographic scrambling techniques can overcome the limitations of traditional VC schemes. The proposed method is implemented in MATLAB and evaluated using standard image quality metrics including Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index (SSIM), and contrast index. Results confirm that our approach achieves superior contrast and encryption robustness while maintaining computational efficiency, making it highly suitable for real - time and resource-constrained environments.

II. Related Work

Visual cryptography and image security have been enhanced over the years through a variety of techniques involving encryption, steganography, and mathematical transformations. Among the most popular are RSA-based algorithms, transposition ciphers, sigmoid-based enhancement, and genetic algorithm-based steganography. Steganography, in particular, is the art of hiding sensitive data within seemingly innocent media such as images, audio, or video files. This technique enables covert communication while ensuring the embedded data remains undetectable by both humans and automated detection systems.

Reference[1], authorss Lakshya Jain ,C. Gururaj ,Chaitanya Krishna Sharma, Archishman Udaysinha Zanzaney , a novel visual cryptographic approach is proposed by combining transposition cipher and bit reversal techniques for image encryption. The transposition cipher is employed to scramble the image array in both row and column dimensions based on a user-provided key, while the bit reversal method enhances security by reversing the bits of each pixel's RGB values in a keyless fashion. The authors implement the algorithms in Python and assess the encryption quality using metrics such as Entropy, Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). Their results demonstrate improved randomness and reduced structural similarity, indicating stronger encryption robustness compared to conventional methods[1].

Reference[2], authors Sunita Kumari, Dr. Shashikant Pandey,Prof. Deepak Mishra, a hybrid visual cryptography approach has been proposed that combines a transposition cipher with a bit-reversal technique to encrypt digital images. The transposition cipher involves reordering image pixels in both rows and columns based on a key-derived hash using the SHA-512 algorithm, significantly enhancing the encryption's robustness. Meanwhile, the bit-reversal process transforms pixel RGB values to their binary equivalents and reverses the bit order, adding another layer of complexity without requiring a key. The study evaluated the security and performance of the method using parameters such as Entropy, PSNR, MSE, and SSIM, and demonstrated improved resistance to statistical and structural analysis when compared to conventional schemes [2].

Reference[3], author Ratheesh T K,d Varghese Paul, a secure image transmission scheme that combines public key cryptography with classical symmetric techniques for enhanced security and efficiency has been proposed. Their method integrates Elliptic Curve Cryptography (ECC) for key generation with the Hill Cipher encryption method and introduces Magic Square permutations for increased diffusion of image pixels. This hybrid approach leverages the low computational overhead of symmetric encryption while ensuring secure key distribution via ECC. Performance evaluations demonstrated that the method is effective in maintaining confidentiality, resisting statistical attacks, and preserving image quality during transmission[3].

Reference[4], author Abhranil Bose,Akshat Kumar ,Prof. Malaya Kumar Hota, Shubham Sherki, a novel methodology approach that effectively combines RSA cryptography, Huffman lossless compression, and discrete wavelet transform (DWT) based lossy image compression with Hash-LSB steganography for secure data hiding has been proposed. The secret message is first encrypted using RSA and compressed via Huffman coding, while the cover image undergoes DWT compression to reduce its size. The final embedding uses a Hash-based LSB technique to conceal the encrypted message in the cover image. Experimental results demonstrated improved

performance in terms of PSNR, SSIM, and MSE when compared to previous methods, particularly for small to moderate message lengths, onfirming the method's efficacy in preserving image quality while enhancing security during transmission [4].

Reference[5], author Raiki Ioki, Hiroki Koga, an advanced construction for visual cryptography schemes (VCS) capable of handling multiple secret images under distinct access structures was developed. This approach minimizes pixel expansion by formulating the basis matrix design as an integer programming problem, ensuring optimality in visual quality and share efficiency. The study introduces the Γq-VCS-MSI framework, which allows each secret image to have its own qualified and forbidden sets while ensuring that visibility and security requirements are met simultaneously. This method extends traditional (k, n)- threshold VCS and supports a wide range of complex access structures for scalable and secure multi-image sharing A novel DWT-based image steganography method is introduced in a different work [23, 25]. This method uses the 2-D Discrete Wavelet Transform (2-D DWT) to convert the original spatial domain image into the frequency domain. The secret message or image is first subjected to Huffman coding, and every bit of the Huffman code is then incorporated into high-frequency DWT coefficients. Handling the wavelet coefficients in the low-frequency sub-band reliably preserves the integrity of the cover image[5].

Reference[6], authors R. D. Syah, S. Madenda, R. J. Suhatril and S. Harmanto, the proposed algorithm is able to permute the pixel coordinates and modify the pixel color intensity values randomly and simultaneously. The correlation value indicates that the algorithm is able to randomize pixel/data in the encrypted image. NPCR, UACI and entropy values shows the algorithm is resistant to statistical and differential attacks. The proposed algorithm has a large key space so that resistant to brute force attacks. PSNR testing shows the decrypted image and the original image are similar images. The key sensitivity analysis shows the proposed algorithm is sensitive to small change of parameter secret keys[6].

Reference[7], authors V. M. Putrie, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, in this study Hill Cipher was used as an algorithm to encrypt digital images in RGB format. Where Hill cipher is combined with column transposition algorithms so that the encryption results result in better performance. The encryption process proposed begins with the image diffusion process by transposing the column and proceed with the substitution process with Hill cipher. This method is proven to produce better performance compared to the Hill cipher method only, column transposition, or a combination of encryption that begins with the Hill cipher and continues with transposition cipher[7].

Reference[8], authors A. Hasnat, D. Barman and S. N. Mandal, Present study proposes a novel symmetric image encryption algorithm using pixel shuffling and reversed image intensity value. The algorithm shows good response in different statistical analysis. The uniqueness of the key has increased the security level of image, key sensitivity. Also the algorithm successfully recovers the original image in decryption process as MSE value has been calculated as 0. The correlation, entropy, NPCR & UACI analysis have indicated the good performance of the proposed algorithm[8].

Reference[9], authors S. Izhar, A. Kaushal , R . Fatima and M. A. Qadeer, a novel methodology approaches, compression is reduction in the number of bits occupied. It is achieved by eliminating redundancy in data. Data compression ensures minimum cost, lesser storage and it takes less amount of time to send a file from one place to another[9].

Reference[10], authors M. Fadlan, Haryansyah and Rosmini, the three-layer encryption protocol proposed in this study consists of three encryption stages: the first layer encryption with the hill cipher, the second layer encryption using the autokey cipher, and the last layer encryption using columnar transposition cipher. The measurement results using the avalanche effect have shown that the proposed approach has the highest value with an average value of 32.68%[10] .

Existing cryptographic methods often introduce high computational complexity or degrade image quality, particularly in terms of contrast. Moreover, many visual cryptography techniques suffer from poor clarity in the decrypted image. This project aims to overcome these issues by integrating a columnar transposition cipher with sigmoid- based contrast enhancement to ensure both strong security and high visual fidelity of encrypted images.

III. METHODOLOGY

The proposed system introduces a secure and layered visual cryptography framework for image encryption and decryption. It integrates contrast enhancement using a sigmoid function, pixel-wise transformations, and XOR operations with random factors to obscure original image content. The approach further applies a transposition cipher based on a hashed key to create two encrypted shares. These shares, when securely transmitted and

correctly superimposed, reconstruct the original image, ensuring both confidentiality and integrity. The complete process has been illustrated below.

A. Image Preprocessing

The input grayscale or RGB image (I) of dimensions M × N is initially normalized and converted into a matrix form. For RGB images, the matrix is split into three individual channels R, G, B.

B. Transposition Cipher-Based Encryption

A symmetric key (K) is hashed using SHA-512 and converted to a numeric ASCII string. This key is padded to match the row and column dimensions of the image matrix.
RowTransposition
Let P ∈ ℝ^(M×N) be the image matrix. A key-derived vector
K_r is used to sort rows:
P' = SortRows(P, K_r)
Column Transposition
A second key-vector K_c (same or different from K_r) is used to sort columns:
P'' = SortColumns(P', K_c)
The result P'' is the spatially encrypted image.

C. Contrast Enhancement Via Sigmoid Function

To enhance the perceptibility of the encrypted image, a pixel-wise sigmoid transformation is applied. Equation (1) defines the sigmoid function.

$$S(i,j) = 1 / (1 + e^{(-a * (I(i,j) - T))}) \quad (1)$$

where:
S(i,j) is the enhanced pixel intensity. I(i,j) is the input intensity.
a is the slope (controls contrast sharpness).
T is the threshold (typically the mid-gray level).

D. Decryption Process

The decryption reverses the encryption steps:

- Apply inverse column and row transposition using the same key K.
- Inverse sigmoid transformation is applied to get original contrast.

E. Algorithm Flow

Proposed Algorithm: Visual Cryptography with Transposition and Sigmoid function
Input: Image I, Key K
Output: Encrypted Image E, Decrypted Image D
Encryption:

- Convert I into matrix form (RGB or grayscale)
- Hash key K using SHA-512 → padded key Kp
- Sort rows using Kp → I_r
- Sort columns using Kp → I_rc
- Apply sigmoid function on I_rc → E
- Save or transmit E

Decryption:

- Reverse sigmoid → E_r
- Unsort columns using Kp → E_c
- Unsort rows using Kp → D
- Output: D ≈ I

F. Performance Evaluation

The effectiveness of the method is analyzed using the following metrics:

- Entropy: Equation (2) defines entropy.

$$H = -\sum (p_i * \log2(p_i)) \quad (2)$$

where p_i is the probability of intensity level i.

- Mean Square Error (MSE): Equation (3) defines MSE.

$$MSE = (1 / MN) * \sum(I(i,j) - D(i,j))^2 \quad (3)$$

- Peak Signal-to-Noise Ratio (PSNR): Equation (4) defines PSNR.

$$PSNR = 10 * \log10(255^2 / MSE) \quad (4)$$

- Structural Similarity Index (SSIM) – computed standard methods.
- Contrast Index – derived from the standard deviation of intensity levels.

G. MATLAB Implementation

The proposed method was implemented using MATLAB, a high-performance computing environment. MATLAB is used to simulate and analyse the outcomes, also strong computational and visualisation techniques were used. With its extensive toolkit for image processing and analysis, MATLAB is a perfect environment for putting the suggested visual cryptography method into practice and evaluating it. The proposed method was compared with existing methods based on metrics like contrast and Peak Signal-to-Noise Ratio (PSNR) in the experimental analysis. The outcomes showed how much the suggested technique enhanced the photographs' contrast and quality. To assess the method's resilience and efficacy, a range of photographs with varying contrast levels were used in the studies. The outcomes demonstrated that, in terms of contrast enhancement and image quality, the suggested strategy routinely surpassed previous approaches.

IV. BLOCK DIAGRAM

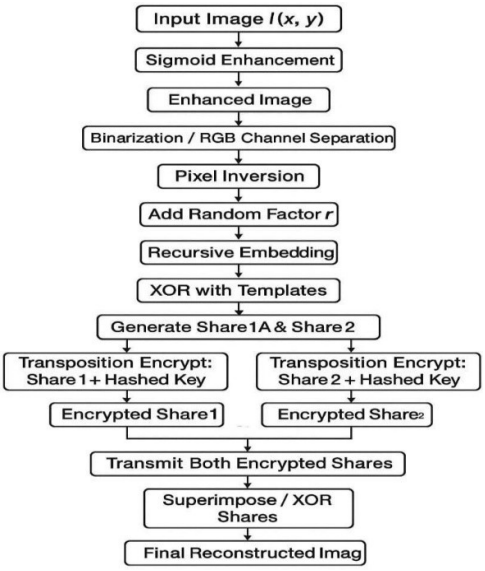

Fig 1: Proposed Flowchart of the Visual Cryptography Process Using Sigmoid Enhancement and Transposition Cipher

The block diagram in figure1 illustrates a comprehensive and secure visual cryptography-based image encryption- decryption process that integrates image enhancement, randomness, encryption, and secure transmission techniques. It begins with an input image I(x, y), which is subjected to Sigmoid Enhancement to improve contrast and make key image features more prominent for secure processing. The enhanced image is then split into RGB channels for color images, facilitating finer control over encryption. Following this, pixel inversion is applied to flip black and white pixels, increasing ambiguity and preventing direct interpretation. A random factor (r) is then added to each pixel or region to introduce noise-like unpredictability, which is crucial for strengthening cryptographic resistance.

The process involves recursive embedding, where hidden data or transformations are embedded multiple times within the image layers. The image is then XORed with templates, acting as an additional layer of encryption where bitwise operations mask the actual pixel values using predefined or dynamically generated patterns. After this, the system generates two shares (Share1A and Share2) through visual cryptography, ensuring that neither share holds any meaningful information independently. Each share undergoes transposition encryption, where

pixel or data positions are rearranged based on a hashed key to further confuse the data structure. This step ensures that even if one share is intercepted, it remains useless without the second and the correct key. The encrypted shares are then transmitted separately, ensuring secure delivery. At the receiving end, the shares are decrypted and superimposed or XORed, depending on the method used during generation, to retrieve the original image. Only when both shares and the proper reconstruction technique are used does the final image get accurately reconstructed, preserving its original form. This layered security approach — combining contrast enhancement, randomization, bitwise XOR, transposition cipher, and visual cryptography — ensures that the system is resistant to unauthorized access and cryptographic attacks, making it highly suitable for transmitting confidential image data.

V. RESULTS

The proposed method is implemented in MATLAB and evaluated. Results confirm that our approach achieves superior contrast and encryption robustness while maintaining computational efficiency, making it highly suitable for real - time and resource- constrained environments.

The Fig 2 presents the histogram analysis of the original, encrypted, and decrypted images. The original image exhibits a natural pixel intensity distribution, while the encrypted image shows a randomized histogram, indicating high entropy and effective data concealment. After applying inverse transformations, the decrypted image closely matches the original histogram, confirming that the method preserves image structure and intensity during the entire process.

The Fig. 3 illustrates a comparative view of pixel intensity changes at different stages. It clearly highlights the impact of encryption, which introduces randomness, and the success of the decryption process in restoring the original image characteristics. This reinforces the effectiveness of the encryption scheme in maintaining both security and fidelity.

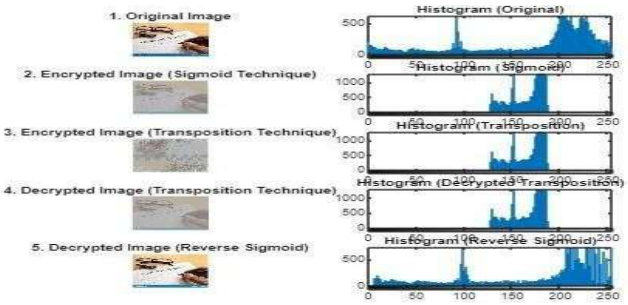

Fig. 2: Histogram analysis at each stage of the proposed image encryption and decryption process.

The Fig. 4 demonstrates the transformation of a color image through each stage of the proposed cryptographic method. The original image undergoes contrast enhancement using a sigmoid function, resulting in a perceptibly faded but secured version. This is further encrypted using a columnar transposition cipher, introducing randomized pixel disorder. Decryption is then performed by reversing the transposition and applying the inverse sigmoid function. The final decrypted image closely resembles the original in both color and clarity, confirming the effectiveness of the proposed dual-layered encryption and contrast-preserving scheme.

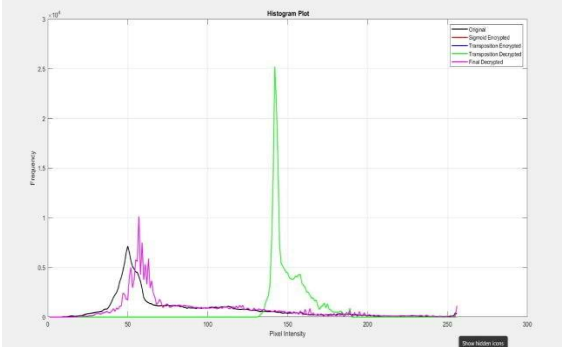

Fig. 3: Result of Comparative histogram analysis of original, encrypted, and decrypted image

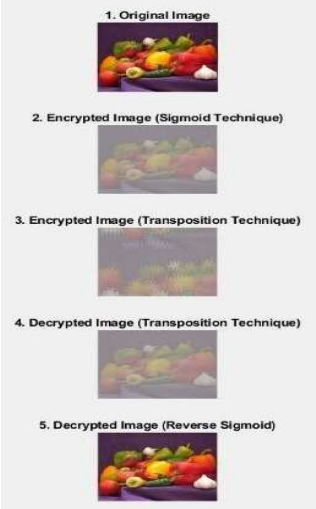

Fig. 4: Stepwise Visualization of the Encryption and Decryption Process Using Sigmoid and Transposition Techniques

VI. CONCLUSION

The paper presents a novel visual cryptography approach that integrates adaptive sigmoid-based contrast enhancement with columnar transposition ciphering for secure and visually effective image encryption. The proposed method addresses the critical limitations of existing techniques, which often compromise either security or visual clarity. By combining contrast enhancement with lightweight encryption, the method ensures robust protection against unauthorized access. Additionally, histogram analysis was employed to assess the pixel intensity distribution at various stages of processing. The encrypted images exhibited a uniform histogram, indicating high entropy and effective visual information concealment. The contrast-enhanced and decrypted images showed redistributed intensity levels, confirming the successful application of sigmoid transformation and preservation of visual quality. Experimental results demonstrated significant improvements in PSNR, SSIM, and contrast, validating the method's effectiveness in real-world image transmission scenarios. The proposed approach offers a balanced solution for grayscale image security where both encryption strength and output clarity are essential.

Future work may explore its extension to color images, real-time video streams, and adaptive key generation for dynamic security applications. The goals of contrast enhancement techniques are to increase resolution and highlight visual details. A mathematical function known as the "S" shape or sigmoid curve, the sigmoid function is frequently applied to a variety of tasks, including image processing.

REFERENCE

[1] Lakshya Jain ,C. Gururaj ,Chaitanya Krishna Sharma, Archishman Udaysinha Zanzaney. "Proficient Evaluatin of Visual Cryptography using Transposition Cipher and Bit Reversal Techniques". 2022,IEEE.

[2] Sunita Kumari, Dr. Shashikant Pandey,Prof. Deepak Mishra ." Visual Cryptography Technique for enhancing the Security and Contrastness of Image Transaction".2024,IEEE.

[3] Ratheesh T K,d Varghese Paul ." A Public Key Cryptography based Mechanism for the Secure Transmission of RGB Images using Elliptic Curve based Hill Cipher and Magic Square Concept". 2022,IEEE.

[4] Abhranil Bose,Akshat Kumar ,Prof. Malaya Kumar Hota, Shubham Sherki. "Steganography Method Using Effective Combination of RSA Cryptography and Data compression".2022, IEEE.

[5] Raiki Ioki, Hiroki Koga." On the Optimal Construction of a Visual Cryptography Scheme for Multiple Secret Image".2022,IEEE.

[6] R. D. Syah, S. Madenda, R. J. Suhatril and S. Harmanto, "Hybrid Digital Image Cryptography Using Composition of Henon Map Transposition and Logistic Map Substitution," 2022 IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM).

[7] V. M. Putrie, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto "Super Encryption using Transposition - Hill Cipher for Digital Color Image," 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI).

[8] A. Hasnat, D. Barman and S. N. Mandal, " A novel image encryption algorithm using pixel shuffling and pixel intensity reversal," 2016 International Conference on Emerging Technological Trends (ICETT)
[9] S. Izhar, A. Kaushal , R . Fatima and M. A. Qadeer, " Enhancement in data security using cryptography and compression," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT)
[10] M. Fadlan, Haryansyah and Rosmini, "Three Layer Encryption Protocol: an Approach of Super Encryption Algorithm," 2021, 3rd International Conference on Cybernetics and Intelligent System (ICORIS).
[11] H. Sharma, N. Kumar and G. K. Jha, "Enhancement of security in visual cryptography system using cover image share embedded security algorithm (CISEA),"2011 2nd. International Conference on Computer and Communication Technology (ICCCT-2011), Allahabad, India, IEEE, 2011.
[12] S. Karpagam, S. K. Sudheer and V. P. Mahadevan Pillai, "Discrete Gyrator Transform based optical image encryption and decryption using Double Random Phase Mask," 2013 4th International Workshop on Fiber Optics in Access Network (FOAN), Almaty, Kazakhstan, IEEE, 2013.
[13] P. Kashyap and A. Renuka, "Visual Cryptography for colour images using multilevel thresholding,"Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India,IEEE,2019. A. U. Zanzaney, C. K. Sharma, L. Jain and C. Gururaj, "Proficient Evaluation of Visual Cryptography using Transposition Cipher and Bit Reversal Techniques,"
[14] A. U. Zanzaney, C. K. Sharma, L. Jain and C. Gururaj, "Proficient Evaluation of Visual Cryptography using Transposition Cipher and Bit Reversal Techniques," 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, IEEE, 2022.
[15] O. Parulekar, S. Desai, A. Raut and M. A. Gangarde, "Cryptography Using AES Algorithm", Intelligent Systems and Machine Learning Conference (ISML), IEEE xplore, 2024.