KUMARAGURU
college of technology
character is life

Journal of image encryption
DOI 27.12.2022

VISUALLY MEANINGFUL IMAGE ENCRYPTION USING RUBIK’S CUBE METHOD AND STEGANOGRAPHY

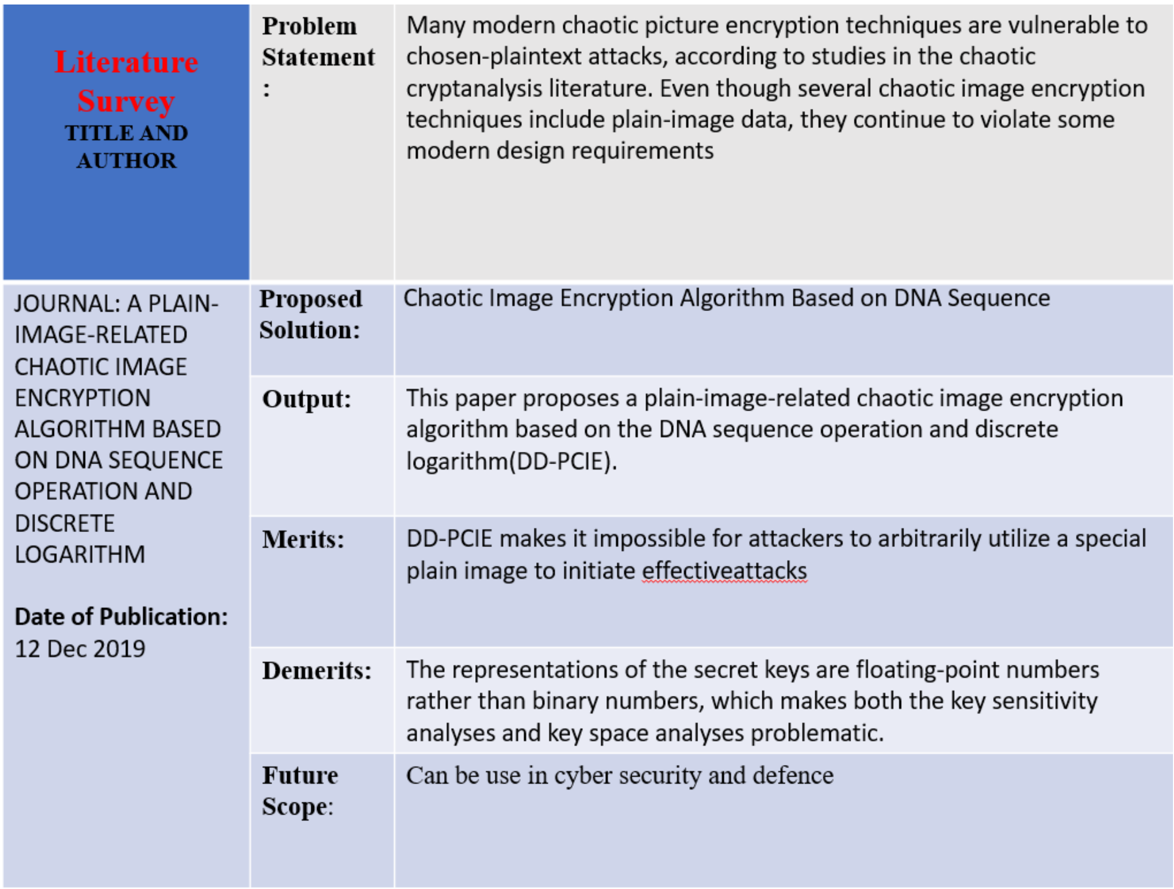
INTRODUCTION

In recent years, with the event of Internet technology and the advent of 5G era, a surging number of individuals use digital images to communicate on the Internet. an outsized quantity of images with secret nature or without authorization are disseminated on the Internet. Since the channel is insecure, various image cryptosystems supported chaos system, cellular automata (CA), SCAN, DNA encoding, quantum computation wave transform are suggested to ensure the security of the image in the transmission process. Cyber-attacks are on the increase. 66% of Chief Audit Executives consider cybersecurity their organization’s greatest 2019 threat. These encryption algorithms typically use relatively small key spaces and thus offer limited security, especially if they're onedimensional. In this paper, we proposed a completely unique image encryption algorithm based on Rubik's cube principle. the first image is scrambled using the principle of Rubik's cube. Then, XOR operator is applied to rows and columns of the scrambled image using two secret keys.

Finally, the experimental results and security analysis show that the proposed image encryption scheme not only are able to do good encryption and perfect hiding ability but also can resist exhaustive attack, statistical attack, and differential attack. Text based encryption is susceptible to cyber threats, creating a vulnerability in their communications. We aim to supply a solution that ensures secure and secret transfer of encrypted communications to prevent readability and identification of those messages and ultimately from falling bait to cybercrime. Steganography has one benefit over cryptography alone: messages don't draw attention to themselves. regardless of how impenetrable, plainly visible encrypted messages may raise suspicion.

Finally, the experimental results and security analysis show that the proposed image encryption scheme not only are able to do good encryption and perfect hiding ability but also can resist exhaustive attack, statistical attack, and differential attack.

LITERATURE SURVEY



Literature Survey TITLE AND AUTHOR	Problem Statement :	Many modern chaotic picture encryption techniques are vulnerable to chosen-plaintext attacks, according to studies in the chaotic cryptanalysis literature. Even though several chaotic image encryption techniques include plain-image data, they continue to violate some modern design requirements
JOURNAL: A PLAIN-IMAGE-RELATED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON DNA SEQUENCE OPERATION AND DISCRETE LOGARITHM **Date of Publication:** 12 Dec 2019	**Proposed Solution:**	Chaotic Image Encryption Algorithm Based on DNA Sequence
	Output:	This paper proposes a plain-image-related chaotic image encryption algorithm based on the DNA sequence operation and discrete logarithm(DD-PCIE).
	Merits:	DD-PCIE makes it impossible for attackers to arbitrarily utilize a special plain image to initiate effectiveattacks
	Demerits:	The representations of the secret keys are floating-point numbers rather than binary numbers, which makes both the key sensitivity analyses and key space analyses problematic.
	Future Scope:	Can be use in cyber security and defence

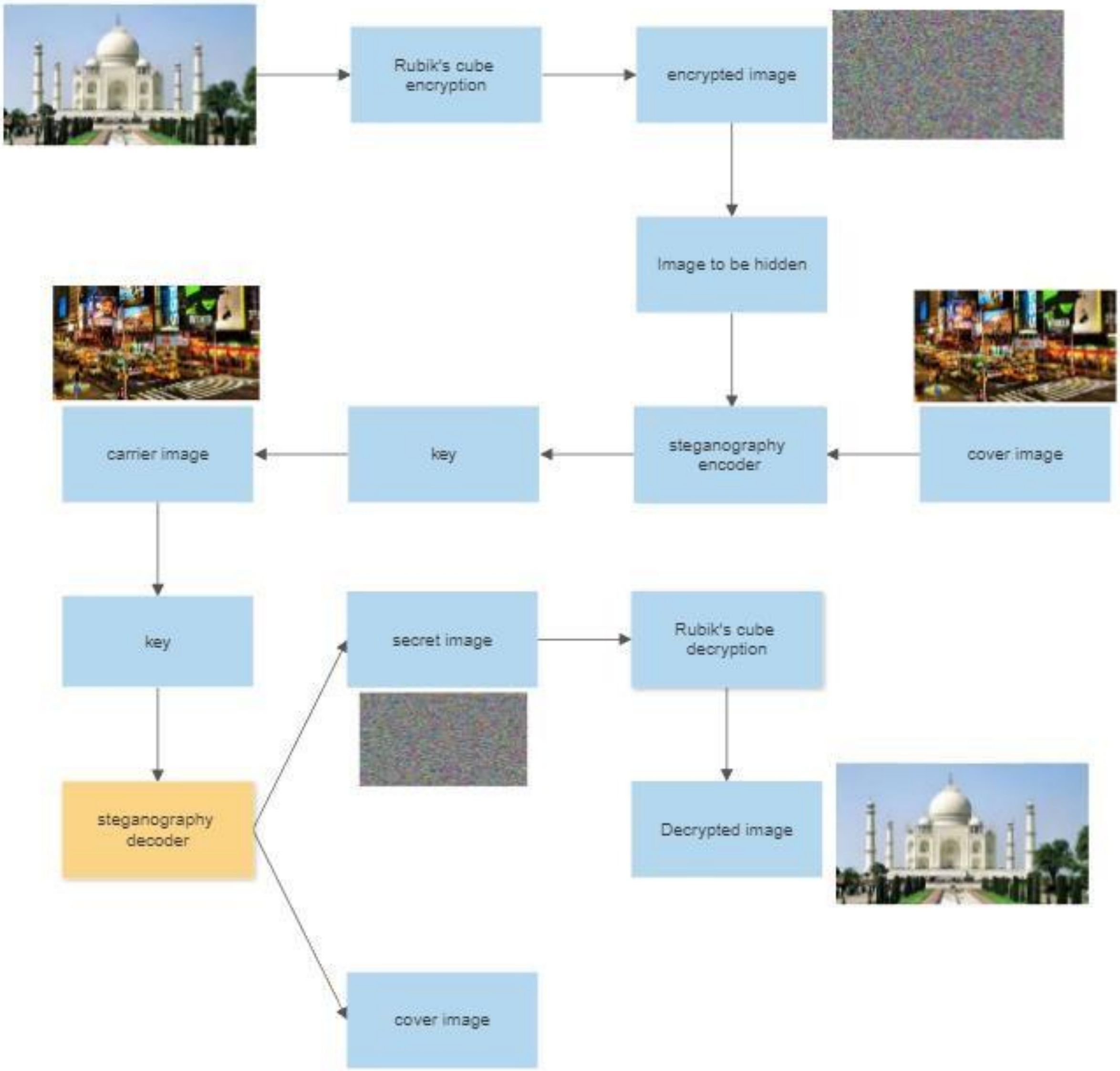
Literature Survey TITLE AND AUTHOR	Problem Statement:	Many modern chaotic picture encryption techniques are vulnerable to chosen-plaintext attacks, according to studies in the chaotic cryptanalysis literature. Even though several chaotic image encryption techniques include plain-image data, they continue to violate some modern design requirements.
JOURNAL: Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public KeyCryptography **Date of Publication:** 19 June 2019	Proposed Solution:	Ghost Imaging and Public Key Cryptography
	Output:	Multiple-image encryption method based on Hadamard basis patterns and RSA public key cryptography is proposed, which solves the problem of low quality of traditional random illumination patterns and increases the security of the system
	Merits:	The detected values including all image information are encrypted by RSA algorithm to obtain the final ⍰ Cipher text, which provides good security for the encryption system. The feasibility, security and multiple-image encryption ability of the proposed method are verified by simulation experiments.
	Demerits:	Hadamard basis patterns is more complex compared to the Fourier single-pixel imaging
	Future Scope:	Cipher text, which provides good security for the encryption system. The feasibility, security and multiple-image encryption ability of the proposed method are verified by simulation experiments.

Literature Survey TITLE AND AUTHOR	Problem Statement:	Many modern chaotic picture encryption techniques are vulnerable to chosen-plaintext attacks, according to studies in the chaotic cryptanalysis literature. Even though several chaotic image encryption techniques include plain-image data, they continue to violate some modern design requirements.
JOURNAL: A Color Image Encryption Algorithm Based on 2D-CIMM Chaotic Map **Date of Publication:** 29 May 2020	Proposed Solution:	2D-CIMM Chaotic Map
	Output:	The 2D-CIMM map simulation results show that it has a wide range of chaos and high SE complexity. Therefore, it is suitable for chaotic image encryption
	Merits:	Results show that it has a wide range of chaos and high SE complexity permutation and diffusion of the encryption process are all performed in bit-level. It enhances the algorithm security
	Demerits:	The diffusion effect is not solely contributed by the diffusion function, the same level of security is achieved in fewer cipher rounds. The encryption speed is thus accelerated
	Future Scope:	enhances the algorithm security and used in cyber security

Literature Survey TITLE AND AUTHOR	Problem Statement:	Many modern chaotic picture encryption techniques are vulnerable to chosen-plaintext attacks, according to studies in the chaotic cryptanalysis literature. Even though several chaotic image encryption techniques include plain-image data, they continue to violate some modern design requirements.
JOURNAL: A New Image Encryption Algorithm for Grey and Color Medical Image **Date of Publication:** 02 March 2021	Proposed Solution:	BLAKE2 hash algorithm, two major operations: confusion and diffusion
	Output:	Encryption is the most straightforward and most efficient method to ensure medical image security via converting the plain image into an unreadable one using a secret key. Without having that secret key, nobody can restore the plain image.
	Merits:	The achieved results show a high-performance security level reached by successful encryption of both grey and color medical images
	Demerits:	A practical algorithm should be susceptible to any slight change to its secret key. Attackers can break the encryption algorithm using a similar key, so any small change in the key used in the decryption step cannot reconstruct the plain image
	Future Scope:	Propose a block and sub block image to accelerate the entire encryption process essential in securing medical images

Literature Survey TITLE AND AUTHOR	Problem Statement:	Many modern chaotic picture encryption techniques are vulnerable to chosen-plaintext attacks, according to studies in the chaotic cryptanalysis literature. Even though several chaotic image encryption techniques include plain-image data, they continue to violate some modern design requirements.
JOURNAL: A Content-Adaptive Joint Image Compression and Encryption Scheme **Date of Publication:** 25 December 2017	Proposed Solution:	We propose a new joint image compression and encryption scheme based on lossy JPEG standard, which aims at encryption power's enhancement, on the premise of maintaining JPEG's compression efficiency.
	Output:	We generate new transforms by introducing rotation angles into order-8 DCT's fwe propose a new joint image compression and encryption scheme based on low-graph structure, and apply them alternatively for 8×8 blocks' transformation, controlled by the encryption key. DC coefficients are encrypted after quantization by 8×8 blocks' permutation and XOR operatio
	Merits:	Data embedding strategy can reduce the cost of sending different 256-bit encryption keys to the decoder when different plain-images are compressed and encrypted
	Demerits:	Currently the encryption scheme cannot achieve perfect correlation removal effect and diffusion property, because the whole encryption work is realized in 8×8 block unit.
	Future Scope:	Can be use in cyber security and defence

PROPOSED METHODOLOGY



A novel encryption algorithm based on the 3-D Rubik's cube is proposed in this paper to achieve 3D encryption of a group of images. This proposed encryption algorithm begins with RC6 as a primary step for encrypting multiple images, separately. Then, the obtained encrypted images are further encrypted with the 3-D Rubik's cube. The RC6 encrypted images are used because the faces of the Rubik's cube. From the concepts of image encryption, the RC6 algorithm adds a degree of diffusion, while the Rubik's cube algorithm adds a degree of permutation. The simulation results demonstrate that the proposed encryption algorithm is efficient, and it exhibits strong robustness and security. The encrypted images are further transmitted over wireless Orthogonal Frequency Division Multiplexing (OFDM) system and decrypted at the receiver side. Evaluation of the standard of the decrypted images at the receiver side reveals good results. The output encrypted image of the Rubik's cube technique is fed as a input for next encryption technique that works on the principle concept of steganography.

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography over cryptography alone is that the intended secret message doesn't attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, regardless of how unbreakable they are, arouse interest and should in themselves be incriminating in countries in which encryption is illegal.

Since we understood the pixel concept and colour models, we will talk about the procedure of hiding an image inside another.

Each pixel has three values (RGB), each RGB value is 8-bit (it means we will store 8 binary values) and the rightmost bits are less significant. So, if we modify the rightmost bits it will have a small visual impact on the final image. this is often the steganography key to hide an image inside another. Change the smaller bits from an image and include the most significant bits from the other image.

Rubik's Cube Algorithm Overview

Given an input image having the three R, G, B matrices of size M X N Hyper parameters include α - used for vector creation ITER_MAX - maximum number of times to carry out operations

A. Encryption

Create two vectors Kr and Kc with |Kr|=M & |Kc|=N. The values of these vectors are randomly picked from 0 to 2α -1

Repeat below steps ITER_MAX number of times

a) Rolling Rows:

1. The sum of all pixel values of every row of the image RGB matrices are calculated one by one.
2. If the sum of a given row number is even, Roll the row to the right Kr [row number] times Otherwise roll to the left Kr [row number] times.

b) Rolling Columns:

1. The sum of all pixel values of every column of the image RGB matrices are calculated one by one.
2. If the sum of a given row column number is even, roll the column up Kc [column number] times. Otherwise roll the column down Kc [column number] times.

c) XORing Pixels:

1. For every pixel(i, j), XOR the pixel with the below two values

Value #1 - Kc [column number] if i is odd else 180 rotated bit version of Kc [column number]

Value #2 – Kr [row number] if j is even else 180 rotated bit version of Kr [row number]

B. Decryption

Given an encrypted image, vectors Kr and Kc & ITER_MAX, decryption can be done by following the reverse procedure - XORing pixels → Rolling Columns → Rolling Rows ITER_MAX number of times

Steganography Algorithm Overview

We can describe a digital image as a finite set of digital values, called pixels. Pixels are the littlest individual element of an image, holding values that represent the brightness of a given colour at any specific point. So we will think of an image as a matrix (or a two-dimensional array) of pixels which contains a fixed number of rows and columns.

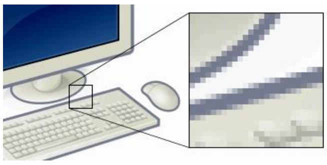


Fig 1

Pixel concept and color models

As already mentioned, pixels are the littlest individual element of an image. So, each pixel may be a sample of an original image. It means, more samples provide more accurate representations of the first. The intensity of each pixel is variable. In color imaging systems, a color is usually represented by three or four component intensities such as red, green, and blue, or cyan, magenta, yellow, and black.

Here, we'll work with the RGB color model. As you'll imagine, the RGB color model has 3 channels, red, green and blue.

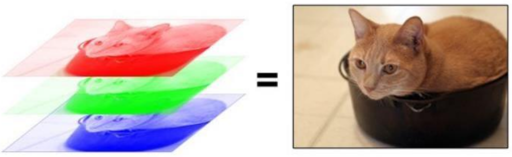


Fig 2

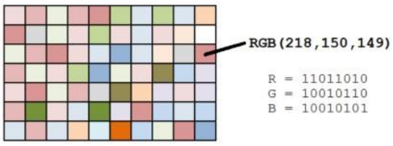


Fig 3

So, each pixel from the image consists of 3 values (red, green, blue) which are 8bit values (the range is 0–255) as shown in fig 1

As we will see in the image above (fig 2), for every pixel we have three values, which may be represented in binary code (the computer language).

The leftmost bit is the most significant bit. If we modify the leftmost bit it will have a large impact on the final value. for instance, if we modify the leftmost bit from 1 to 0 (11111111 to 01111111) it will change the decimal value from 255 to 127.

On the opposite hand, the rightmost bit is the less significant bit. If we modify the rightmost bit it will have less impact on the final value. for

instance, if we modify the leftmost bit from 1 to 0 (11111111 to 11111110) it will change the decimal value from 255 to 254. Note that the rightmost bit will change just one in a range of 256 (it represents less than 1%).

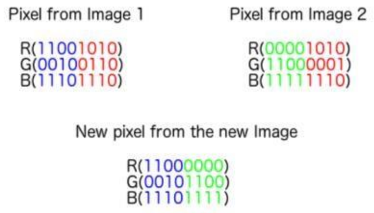


Fig 4

HARDWARE AND SOFTWARE REQUIREMENTS

- Python 3.9
- Open CV
- Pillow
- Numpy

PERFORMANCE ANALYSIS

The experiments that were run to evaluate the effectiveness and security of the suggested picture encryption technique are presented in this part. Visual testing and security analysis are part of these exams.

Visual Testing

For visual testing, four gray-scale images of size 256×256 pixels were used. Figure 1 depicts these test images as well as the images encrypted using the proposed Rubik's cube algorithm. From this figure, one can see that there is no perceptual similarity between original images and their encrypted counterparts.

Security Analysis

Security is a significant problem in cryptology. Known plain text attacks, cipher-textonly attacks, statistical analysis attacks, and brute-force attacks are a few examples of attacks that a decent picture encryption method should be able to fend off. This section does a security analysis on the suggested technique for picture encryption. On the basis of key space analysis and statistical analysis, security was evaluated.

Statistical Analysis

Shannon wrote in a 1949 study [17] that "Many forms of cyphers can be solved by statistical analysis." Therefore, in order to defend against potent attacks based on statistical analysis, he proposed two strategies based on confusion and diffusion. In the current study, statistical research has been carried out to show the suggested encryption algorithms better confusion and diffusion features against statistical attacks. This is accomplished by running two different sets of tests, including the computing of correlations between neighboring pixels in encrypted images and the examination of histograms in encrypted images.

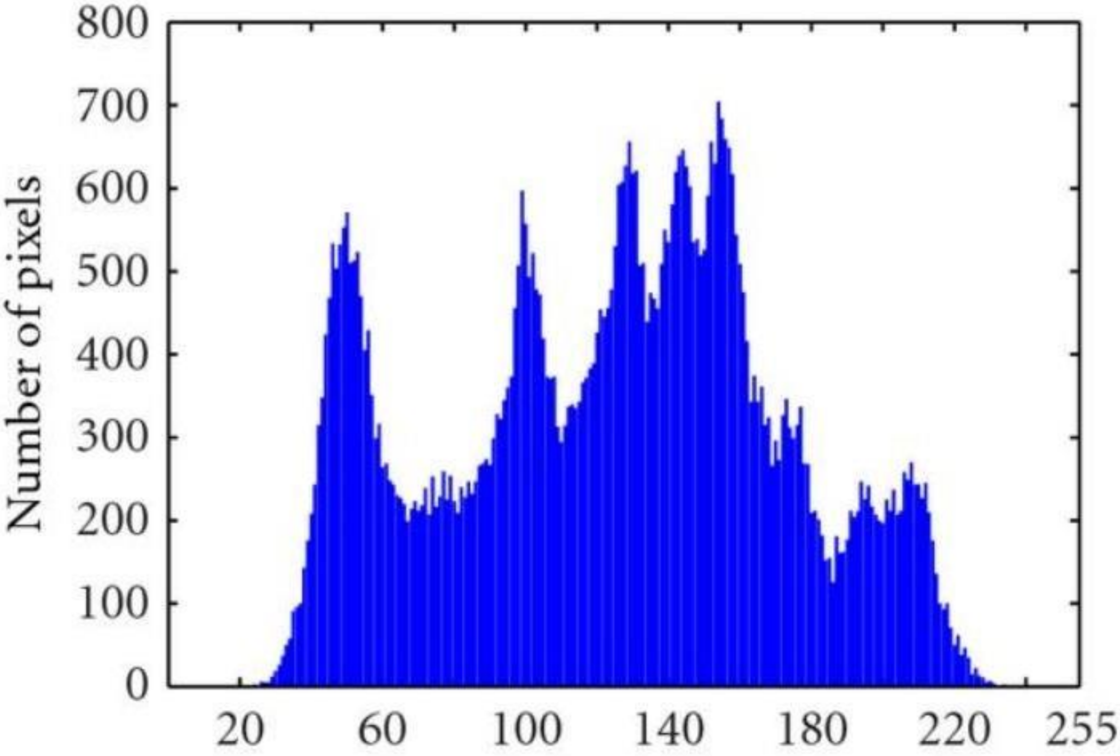


Fig 5: Original image

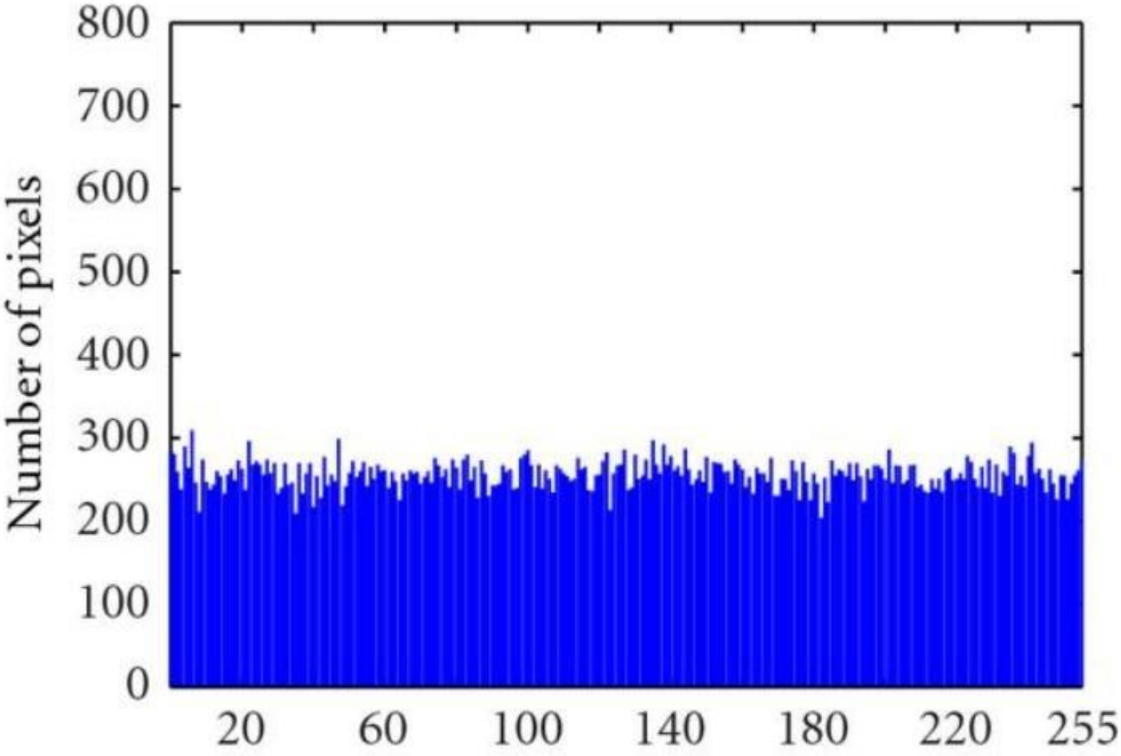
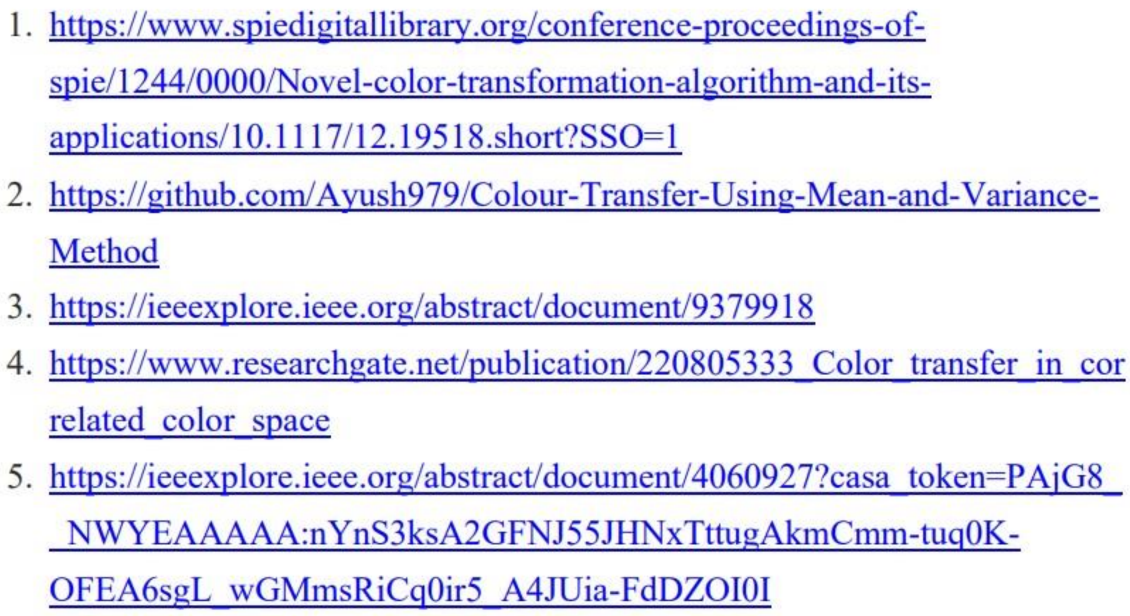


Fig 6: Encrypted image

CONCLUSION

This study proposes a method for image encryption based on Rubik's Cube Principle and Steganography. Different measurement matrices can be utilised in the CS stage to measure each column of the picture signal by selecting a random quantity. Even though the same image is used, various random numbers can be chosen to create distinct secret images. The secret key remains the same. CS has assisted in advancing the stage of by embedding, the carrier image can be lower in size. Compared to the plain image when using the block pairing approach and there is no need for more bandwidth because replacement is applied in the transfer. The method features a wide key space, high key sensitivity, and decent robustness against common assaults, according to simulation findings and security assessments.

REFERENCE



1. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/1244/0000/Novel-color-transformation-algorithm-and-its-applications/10.1117/12.19518.short?SSO=1
2. https://github.com/Ayush979/Colour-Transfer-Using-Mean-and-Variance-Method
3. https://ieeexplore.ieee.org/abstract/document/9379918
4. https://www.researchgate.net/publication/220805333_Color_transfer_in_correlated_color_space
5. https://ieeexplore.ieee.org/abstract/document/4060927?casa_token=PAjG8__NWYEAAAAA:nYnS3ksA2GFNJ55JHNxTttugAkmCmm-tuq0K-OFEA6sgL_wGMmsRiCq0ir5_A4JUia-FdDZOI0I