

**IMAGE ENCRYPTION USING RUBIK’S CUBE METHOD AND STEGANOGRAPHY**

# 

# A PROJECT REPORT

***Submitted by***

**BHARATH S (20BCS020)**

**KAVIMANI S (20BCS053)**

**BADHRINATHAN S B (20BCS019)**

**HARI PRASAD N M (20BCS036)**

**AKSHATHAA A S (20BCS007)**

***In partial fulfillment for the award of the degree***

*of*

**BACHELOR OF ENGINEERING**

in

**COMPUTER SCIENCE AND ENGINEERING**

**KUMARAGURU COLLEGE OF TECHNOLOGY**

**COIMBATORE-641 049**

(An Autonomous Institution Affiliated to Anna University, Chennai)

**DECEMBER 2022**

 **KUMARAGURU COLLEGE OF TECHNOLOGY**

**COIMBATORE 641 049**

(An Autonomous Institution Affiliated to Anna University, Chennai)

**BONAFIDE CERTIFICATE**

Certified that this project report **“IMAGE ENCRYPTION USING RUBIKS CUBE METHOD AND STEGANOGRAHY”** is the bonafide work of **“BHARATH S (20BCS020),KAVIMANI S (20BCS053),BADHRINATHAN S B (20BCS019),HARIPRASAD N M (20BCS036), AKSHATHAA A S (20BCS007)**  who carried out the project work under my supervision.

|  |  |
| --- | --- |
| **SIGNATURE** | **SIGNATURE** |
| **Dr. Devaki. P, Ph.D.,** | **Mr. V. Senthil Kumar, Assistant**  **Professor** |
| **HEAD OF THE DEPARTMENT** | **SUPERVISOR** |
| Department of Computer Science and Engineering, | Department of Computer Science and  Engineering, |
| Kumaraguru College of Technology | Kumaraguru College of Technology |
| Coimbatore – 641 049 | Coimbatore – 641 049 |

The candidates with University register number **20BCS020, 20BCS053, 20BCS019, 20BCS036, 20BCS007** were examined in the Project Viva-Voice examination held on 31.12.2022.

Internal Examiner External Examiner

**DECLARATION**

We affirm that the project work titled **“IMAGE ENCRYPTION USING RUBIKS CUBE METHOD AND STEGANOGRAPY”** being submitted in partial fulfilment for the award of B.E Computer Science and Engineering is the original work carried out by us. It has not formed the part of any other project work submitted for the award of any degree or diploma, either in this or any other University.

**BHARATH S (20BC020) KAVIMANI S (20BCS053)**

**BADHRINATHAN S B (20BCS019) HARIPRASAD N M(20BCS056)**

**AKSHATHAA A S (20BC007)**

I certify that the declaration made above by the candidates are true.

# Mr. V. Senthil Kumar,

Assistant Professor,

Department of Computer Science and Engineering,

Kumaraguru College of Technology,

Coimbatore – 641 049.

**ACKNOWLEDGEMENT**

We express our profound gratitude to the management of Kumaraguru College of Technology for providing as with the required infrastructure that enabled us to successfully complete the project.

We extend our gratefulness to our Principal, **Dr. Saravanan D,** for providing us the necessary facilities to pursue the project.

We would like to acknowledge **Dr. P. Devaki,** Professor and Head, Department of Computer Science and Engineering, for her support and encouragement throughout this project.

We thank our project coordinator **Dr.L.Latha,** Professor, Department of Computer Science and Engineering and guide **Mr. V. Senthil Kumar,** Assistant Professor, Department of Computer Science and Engineering, for their constant and continuous effort, guidance and valuable time.

Our sincere and hearty thanks to staff members of Department of Computer Science and Engineering of Kumaraguru College of Technology for their well wishes, timely help and support rendered to us during our project. We are greatly indebted to our family, relatives and friends, without whom life would have not been shaped to this level.

# TABLE OF CONTENTS

**CHAPTER TITLE PAGE NO.**

**NO.**

**ABSTRACT** 2

# 1 INTRODUCTION 3

1.1 CONCEPTUAL STUDY OF THE PROJECT 4

1.2 OBJECTIVES OF THE PROJECT 4

1.3 SCOPE OF THE PROJECT 5

1. **LITERATURE REVIEW**

2.1 LITERATURE REVIEW OF JOURNALS 6

1. **PROBLEM DEFINITION**

# 4 PROPOSED SYSTEM 12

4.1 BLOCK DIAGRAM 13

4.2 METHODOLOGY 14

4.3 IMPLEMENTATION 17

1. **SYSTEM REQUIREMENTS** 17

5.1 REQUIREMENTS 17

1. **CONCLUSION** 18
2. **APPENDIX** 18

# ABSTRACT

Image encryption play a major role in security and information transfer. This is because there are high possibility for large number of attack and hacking of secret images transferred in various sector .Most of the encryption techniques used in present days are either high complex or use simple encode key that can easily be cracked. So the encode key for encryption should be less complex and difficult to crack. Here we developed an algorithm which is uses a less complex rubix cube algorithm and steganography to make it difficult to crack it.

**1. 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

## 1.1 CONCEPTUAL STUDY OF THE PROJECT

The end of the 20th century was marked by an extraordinary technical revolution from analog to numerical as documents and equipments became increasingly used in various domains. However, the advantages of the digital revolution were not achieved without drawbacks such as illegal copying and distribution of digital multimedia documents. To meet this challenge, researchers were motivated more than ever to protect multimedia documents with new and efficient document protection techniques. In this context, different techniques have been introduced such as encryption and digital watermarking. The first one consists in transforming

multimedia documents using an algorithm to make it unreadable to anyone except for the legitimate users. The second one consists of embedding digital watermarks into multimedia documents to guarantee the ownership and the integrity of the digital multimedia contents. The protection of images is of particular interest in

this paper. Traditional image encryption algorithms such as private key encryption standards (DES and AES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC), as well as

the international data encryption algorithm (IDEA), may not be the most desirable candidates for image encryption, especially for fast and real-time communication applications. In recent years, several encryption schemes have been proposed [1–12]. These encryption schemes can be classified into different categories such as value transformation,pixels position permutation , and chaotic systems .

## 1.2 OBJECTIVES OF THE PROJECT

In the past few years, several encryption algorithms based on chaotic systems have been proposed as means to protect digital images against cryptographic attacks. These encryption algorithms typically use relatively small key spaces and thus offer limited security,especially if they are one-dimensional. In this paper, we proposed a novel image encryption algorithm based on Rubik’s cube principle. The original 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 can achieve good encryption and perfect hiding ability but also can resist exhaustive attack, statistical attack, and differential attack.

## 1.3 SCOPE OF THE PROJECT

Image security should be paid much attention in order to combat illegal access, revision, and other attacks. In recent years, many image encryption algorithms have been proposed and published, for example, chaos-based methods, compressive sensing-based schemes, quantum map-based algorithms, etc.  
  
Image recognition powered by deep learning can provide us advance capabilities like personalized searches, customer analytics, social media and conversation commerce, etc. With the date they got from image recognition, businesses can find insights for campaigns and marketing strategies.  
  
Steganography is a useful tool that allows covert transmission of information over an over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval.

# 2. LITERATURE REVIEW

**1. JOURNAL: A PLAIN-IMAGE-RELATED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON DNA SEQUENCE**

**OPERATION AND DISCRETE LOGARITHM**

**PUBLISHED: Digital Object Identifier**

**ABSTRACT:**

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. Consequently, after reviewing numerous literatures on chaotic image encryption, we suggest a Deoxyribonucleic acid (DNA)based chaotic image encryption technique for plain images a discrete logarithm and procedure. We are aware that the discrete logarithm calculation is a difficult nonlinear process. Calculation can make encryption more difficult if it is introduced. More importantly, discrete Varied generators produce drastically different logarithm values, and the multiplicative group used. There can be as many as 128 generators in the suggested approach.

**REFERENCE:** WEI FENG, YIGANG HE, HONGMIN LI , CHUNLAI LI

**DATASETS**: Kodak Dataset

**PROPOSED MODEL**: Chaotic Image Encryption Algorithm Based on DNA

Sequence

**REVIEW:**

This paper proposes a plain-image-related chaotic image encryption algorithm based on the DNA sequence operation and discrete logarithm (DD-PCIE). In each step of its encryption process, DD-PCIE not only utilizes the hash value of the plain- image to enhance its plain-image sensitivity and plain-image relevancy, but also introduces the discrete logarithm to improve the complexity of its encryption process. Therefore, DD-PCIE can effectively resist chosen-plaintext attack.

**PROS:**

* DD-PCIE applies the discrete logarithm and the hash value of the plain- image to the whole encryption process, thus greatly improving its ability to resist chosen-plaintext attack.
* DD-PCIE makes it impossible for attackers to arbitrarily utilize a special plainimage to initiate effective attacks.
* DD-PCIE also expands the key space and increases the complexity and plainimage relevancy of the encryption process, thus further improving its security

**CONS:**

* 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.
* One-time pad (OTP) secret key designs are not practical in applications where a large number of images need to be encrypted.

**2. JOURNAL: A NOVEL COLOR IMAGE ENCRYPTION ALGORITHM**

**BASED ON THREE-DIMENSIONAL CHAOTIC MAPS AND**

**RECONSTRUCTION TECHNIQUE**

**PUBLISHER: Digital Object Identifier**

**ABSTRACT:**

Using three-dimensional chaotic maps and a few data reconstruction techniques, the research proposes a novel color image encryption approach. The three-dimensional chaotic logistic map is introduced in the encryption algorithm's diffusion process to alter the pixel value of the plain image. The three-dimensional chaotic Cat map is used in the confusion process to cope with the placement of the image pixels. Additionally, several data reconstruction techniques are used to improve the encryption outcome. Also included is the matching decryption algorithm. The effectiveness and simplicity of our approach are its primary benefits, and it effectively breaks the correlation between picture pixel layers, provides a wide key space, and defends against differential and statistical attacks.

**REFERENCE:** JI XU1 , CHEN ZHAO 1,2, AND JUN MOU 1,2

**DATASETS**: D-90, Kodak dataset

**PROPOSED MODEL**: Three-Dimensional Chaotic Maps and Reconstruction

Technique

**REVIEW:**

The high-dimensional chaotic maps and some data reconstruction techniques have been applied to achieve a novel encryption algorithm for color images of any size. In the diffusion process of the encryption algorithm, the three-dimensional chaotic Logistic map is introduced to changes the pixel value of the plain image. Meanwhile, in the confusion process, the three-dimensional chaotic Cat map is applied to deal with the position of the image pixels

**PROS:**

* Our proposed method breaks the correlation between image pixel layers, offers

a large key space and against differential and statistical attacks effectively.

* This encryption algorithm has a fast encryption speed.

**CONS:**

* The logistic map has the disadvantages of uneven distribution, low security, and small parameter space.

**3. JOURNAL: An Image Encryption Algorithm Based on BP Neural Network and Hyper chaotic System**

**ABSTRACT:**

To increase the secure transfer of information while lowering the bandwidth and storage requirements for image information. This research proposes an image reduction and encryption algorithm based on BP neural network and fractionalorder memristive hyperchaotic system. In this approach, the fractional-order memristive hyperchaotic system is utilised to diffuse the pixel values after the BP neural network compresses the image's pixel values. The outcomes of the experimental simulation show that the suggested approach has stronger security features in addition to being able to properly compress and encrypt images. The safe transmission and storage of image information in practical communication is thus supported by this work's theoretical recommendations and experimental foundation.

**PUBLISHED: Digital object Identifier**

**REFERENCE**: Feifei Yang, Jun Mou , Yinghong Cao, Ran Chu

**DATASETS:** Kodak dataset

**PROPOSED MODEL:** BP Neural Network and Hyper chaotic System

**REVIEW:**

The results show that the mean NPCRs and UACIs of the proposed algorithm are close to the theoretical value of 99.6% and 33.3% respectively. Therefore, the algorithm can resist the differential attack.

**PROS:**

The proposed image compression and encryption algorithm is an effectively method for the safe transmission of image information in practical communication applications.

**CONS:**

Data loss and noise attacks can occur at some situations

**4. JOURNAL: Meaningful Encryption: Generating Visually**

**Meaningful Encrypted Images by Compressive Sensing and Reversible Color Transformation**

**PUBLISHED: Digital Object Identifier**

**ABSTRACT:**

In the field of information security, compressive sensing (CS) and visual security (VS) have recently attracted academics' interest. The measurement matrix, however, is frequently utilised in CS, which leaves it open to a specific plaintext attack (CPA). Additionally, the size of the cypher used to create meaningful cypher images often equals or exceeds the size of the simple picture for the carrier image. To get around these limitations. It is suggested to use CS and reversible colour modification to create a new, visually secure image encryption technique. The approach is composed of two steps: embedding and compression. Chaotic sequence is present in the initial stage. utilised to produce various architecturally random matrices.

A random number is inserted during the sampling procedure when CS is used. Different measurement matrices can be used to compress and encrypt the same image in different orders by selecting various random values. To create a meaningful image in the second stage, block pairing, colour transformation, and block replacement are used. This study initially tries to replace the carrier image's block with a compressed noise-like image block, which is different from the block replacement between two similar images. As a result, the carrier picture can be smaller than the plain image, saving transmission bandwidth. The suggested encryption system has strong encryption performance, can successfully fend off common assaults, and is appropriate for meaningful image encryption, according to theoretical analysis and experimental findings.

**REFERENCE**: PING PING 1 , JIE FU 1, YINGCHI MAO 1 , FENG XU 1 , AND JERRY GAO 2

**DATASETS:** Real CFA, Standard image

**PROPOSED MODEL:** Compressive sensing, Reversible Color transformation

**REVIEW:**

The simulation results and security analysis show that the scheme has large key space, high key sensitivity and good robustness against common attacks.

**PROS:**

The size of cipher image is related to encryption time and transmission bandwidth, so smaller size can improve encryption efficiency and transmission speed.

**CONS:**

Complex mathematical formulas are included in the implementation of the model.

**5. JOURNAL: Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography**

**PUBLISHED: Digital Object Identifier**

**ABSTRACT:**

This work suggests a multiple-image encryption system based on ghost imaging that combines public key cryptography and the Hadamard basis pattern. The Hadamard basis patterns are utilised for illumination and a number of light paths are set up in the encryption system so that each light path is concentrated in a bucket detector to acquire intensity values for all images. The final ciphertext is then generated by encrypting all of the detected intensity values using a public key cryptography technique. Reconstruction can be done with high-quality by using basis patterns.

Public key cryptography and randomization in the permutation operation also give the encryption system a significant security feature. The crosstalk issue between images is resolved by the multiple-image encryption approach. The feasibility and security of the suggested method are confirmed by numerical simulation after the fundamental principle of the encryption system has been theoretically studied.

**REFERENCE:** Leihong Zhang , Xiao Yuan, Kaimin Wang, Dawei Zhang

**DATASETS:** Standard Image

**PROPOSED MODEL:** Ghost Imaging and Public Key Cryptography

**REVIEW:**

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

**PROS:**

* 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.

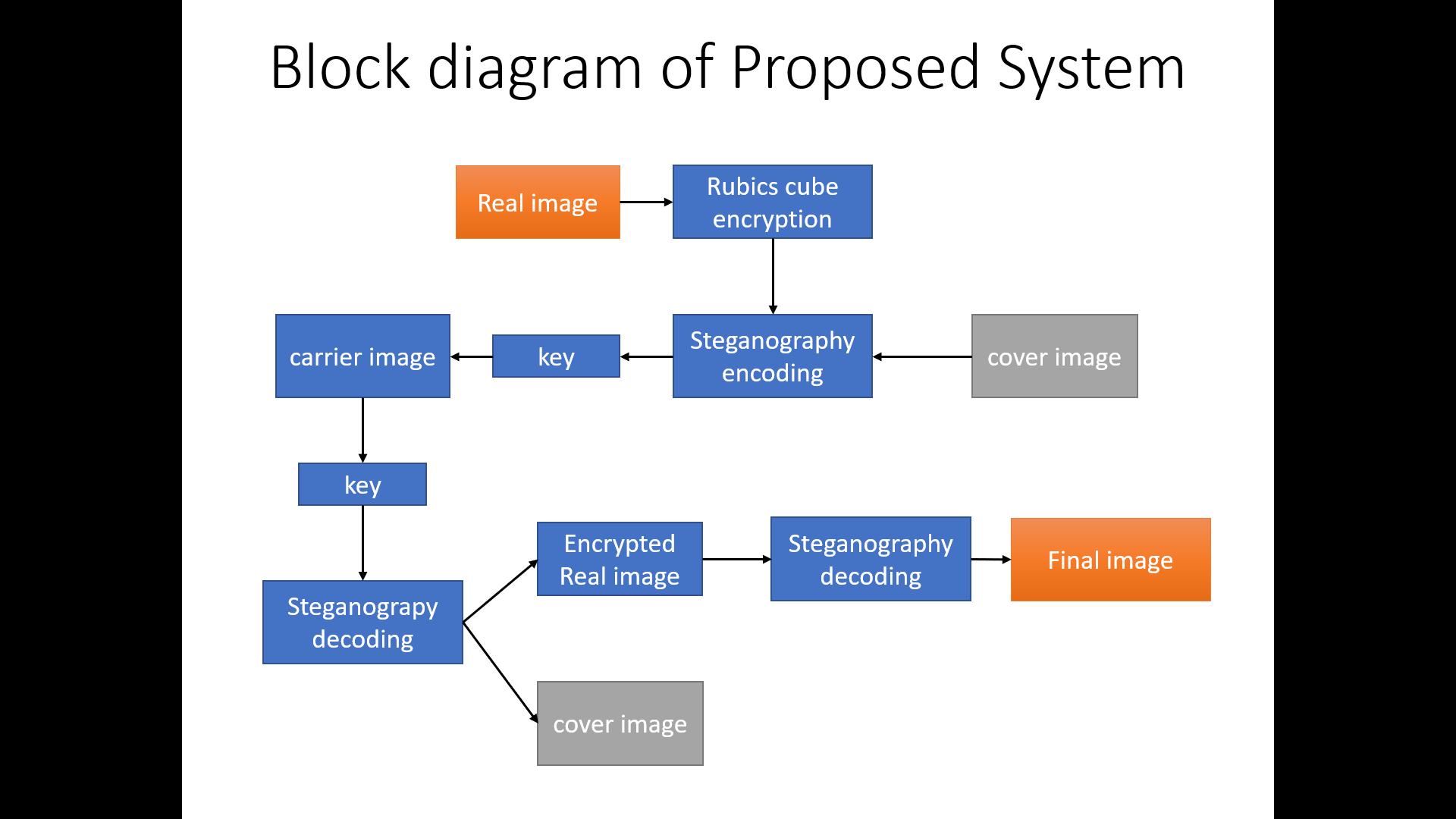
**CONS:**

Hadamard basis patterns is more complex compared to the Fourier single-pixel imaging.

# 4. PROPOSED SYSTEM

In this paper we have developed an algorithm which is used to encrypt a image using rubiks cube method and covers it with a cover image using steganography. This can be done on an image of different size ,resolution and type(.jpg or .png).

## 4.1. BLOCK DIAGRAM



Rubixs cube decryption

## 4.2. 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

1. 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.
2. 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.
3. 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]

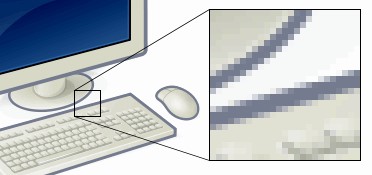
Value #2 – Kr [row number] if j is even else 180 rotated bit version of Kr [row number]

### 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

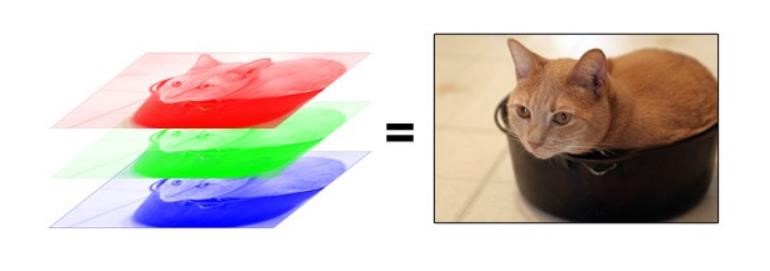
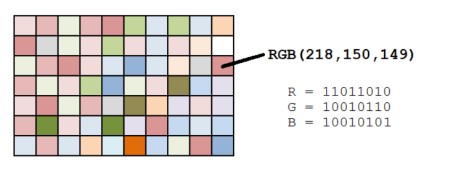
We can describe a digital image as a finite set of digital values, called pixels. Pixels are the littlest individual element of an image, holding values that represent the brightness of a given colour at any specific point. So we will think of an image as a matrix (or a two-dimensional array) of pixels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



**Pixel concept and color models** *Fig 1*

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 3*

*Fig 2*

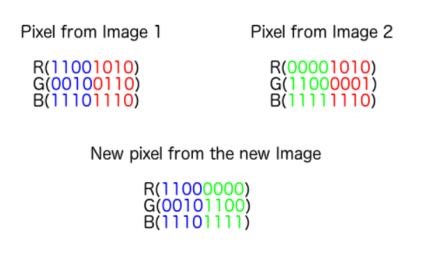
So, each pixel from the image consists of 3 values (red, green, blue) which are 8bit values (the range is 0–255) as shown in fig 1

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

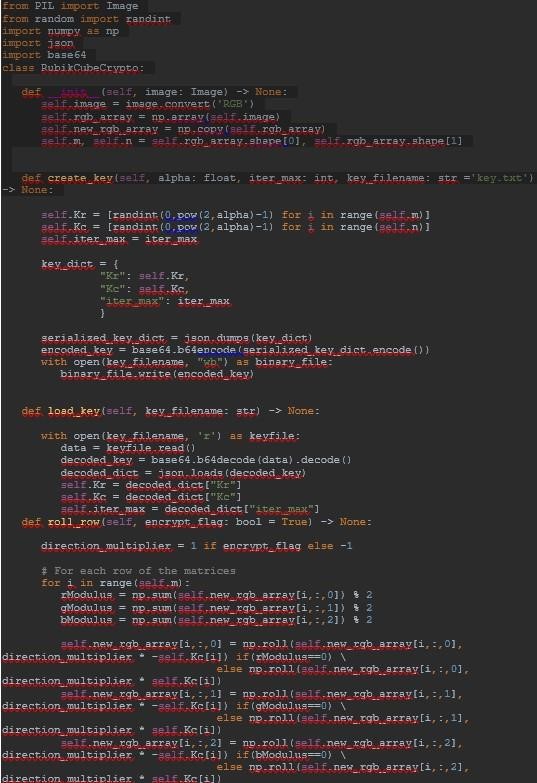
instance, if we modify the leftmost bit from 1 to 0 (11111111 to 11111110) it will change the decimal value from 255 to 254. Note that the rightmost bit will change just one in a range of 256 (it represents less than 1%).

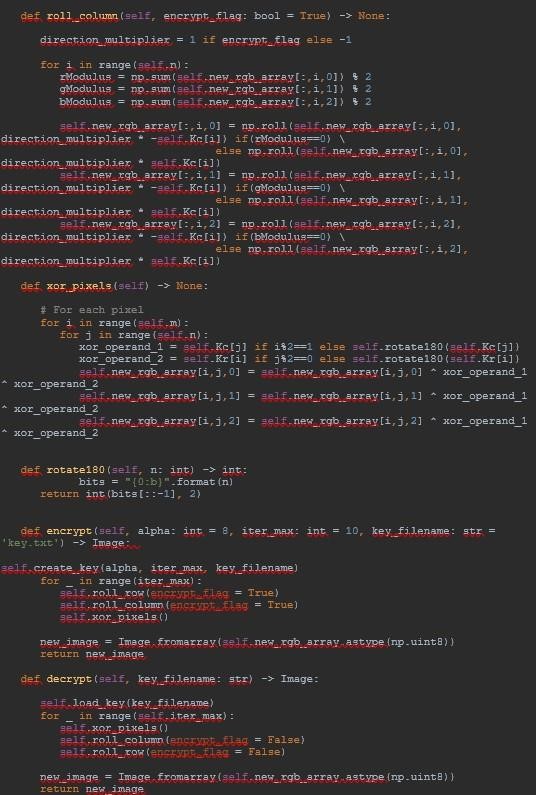


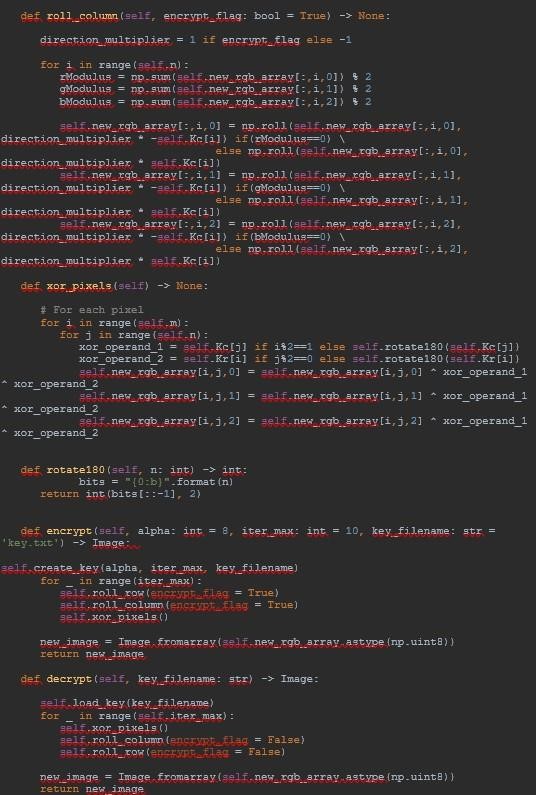
# 6. CONCLUSION

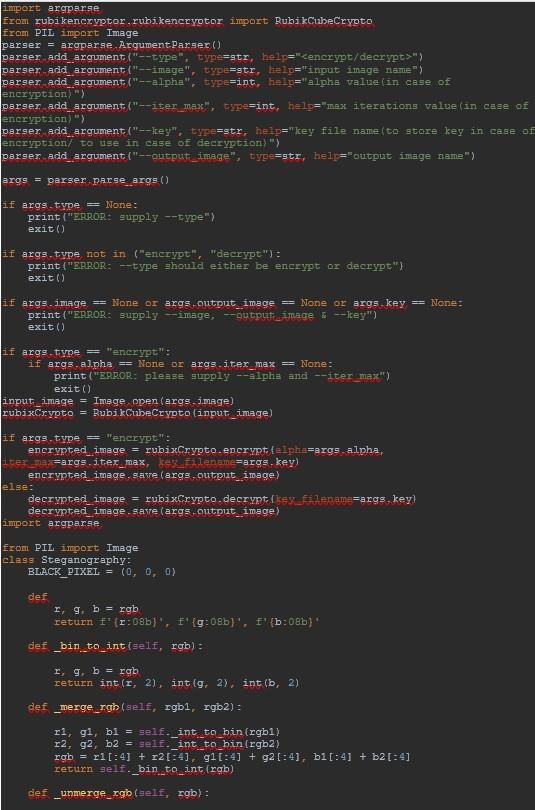
This study proposes a method for image encryption based on Rubik's Cube Principle and Steganography. Different measurement matrices can be utilised in the CS stage to measure each column of the picture signal by selecting a random quantity. Even though the same image is used, various random numbers can 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.

# 7.APPENDIX: sample setup



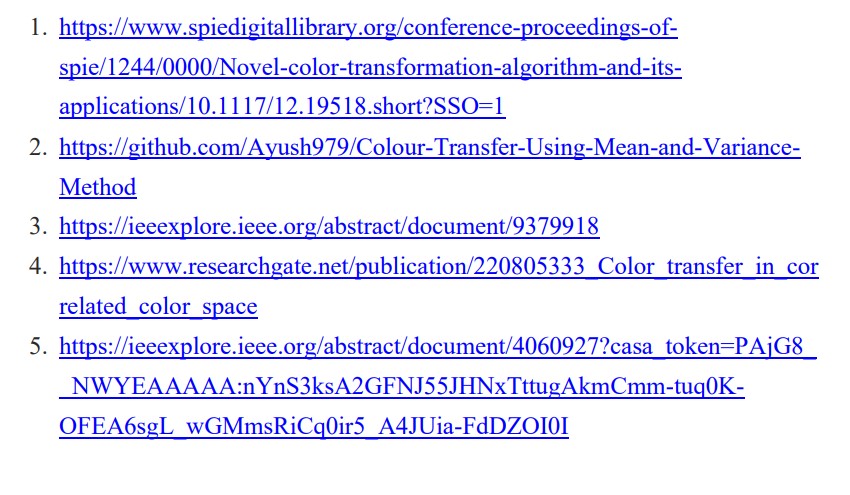








# REFERENCES



JOURNEL LINK:

[JOURNEL ON IMAGE ENCRYPTION](https://drive.google.com/file/d/1oXE7KETDIeoZzrQtNY2TOriE4R01RDRd/view?usp=share_link)