A MAJOR PROJECT-II REPORT

ON

IMAGE ENCRYPTION AND DECRYPTION USING RUBIK'S CUBE PRINCIPLE

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY (M. TECH)

IN

COMPUTER SCIENCE & ENGINEERING

Submitted by

AMIT CHAHAR

2K22/CSE/03

Under the Supervision of

Prof. Manoj Kumar

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042
MAY, 2024

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, **Amit Chahar, 2K22/CSE/03** students of M.Tech. in Computer Science and Engineering, hereby declare that the project Dissertation titled "**Image Encryption and Decryption Using Rubik's Cube Principle**" which is submitted by me to the **Department of Computer Science and Engineering, Delhi Technological University, Delhi** in partial fulfilment of the requirement for the award of degree of **Master of Technology** in **Computer Science and Engineering**, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: **Delhi** **Amit Chahar**
Date: **2K22/CSE/03**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled "**Image Encryption and Decryption Using Rubik's Cube Principle**" which is submitted by **Amit Chahar, 2K22/CSE/03**, **Department of Computer Science and Engineering**, **Delhi Technological University, Delhi** in partial fulfilment of the requirement for the award of the degree of **Master of Technology** in **Computer Science and Engineering**, is a record of the project work carried out by the student under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: **Delhi** **Prof. Manoj Kumar**
Date:

ABSTRACT

It is more important than ever to protect privacy and safeguard data in a world that is changing quickly. New and improved technologies and algorithms are always being developed and tested for safe text, picture, and video communication. This thesis uses Rubik's Cube technology to provide a revolutionary method of safe encryption and decryption of coloured pictures. By transforming picture pixels using the principles of Rubik's Cube, the suggested approach ensures strong encryption against a variety of parametric and analytical assaults. The method's suitability for real-time Internet protection has been assessed, and it has proven to be very secure and efficient. This work advances the field of data security by offering a sophisticated and dependable technique for both encrypting and decrypting pictures with colour.

Keywords: Advanced, Secure, Coloured Images, Rubik's Cube Algorithm, Encryption, Decryption

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I wish to express my sincerest gratitude to **Prof. Manoj Kumar** for his continuous guidance and mentorship that he provided us during the project. His direction helped me understand and accomplish my objectives, emphasizing the significance and industrial relevance of this project. He was always available to assist and clarify any doubts we encountered. This project would not have been successful without his continuous support and encouragement.

I would like to extend my sincere thanks to **"Prof. Vinod Kumar"**, *Head of Department*, Department of Computer Engineering, Delhi Technological University, Delhi for his valuable suggestions and feedback on our project work.

Finally, I would like to thank all the participants who participated in the study, without whom this research would not have been possible. I express my sincere gratitude to all the individuals who have directly or indirectly contributed to the success of my project.

Amit Chahar
(2K22/CSE/03)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Overview

Towards the end of the 20th century, a remarkable technological revolution from the analog to the digital was witnessed, as apparatus and paper-work were increasingly used in a diverse context of areas. The benefits of the digital revolution did not, however come all that free of charge – a fact played out by the illegal sharing and copying of digital multimedia resources. Now, more than ever, academicians are forced to make working and feasible document security systems to solve a problem of multimedia document security. A few methodologies were introduced in this area: digital watermarking and encryption. Actually, the first one includes an application of an algorithm to change the multimedia content so as to permit only authorized users to read them. The second approach is digital watermarking, which has an idea of inseparably inserting watermarks into multimedia documents to assure the integrity and ownership of the digital multimedia materials.

We are particularly interested in image protection in this work. IDEA, ECC, and RSA, along with the traditional image encryption algorithms like DES and AES, may not be of optimum suitability for the purpose of image encryption, particularly for the quick and real-time communication applications. An image encryption approach using repetitive random phase encoding in gyrator transform domains was reported by Liu et al. Iterative random phase encodings use two-dimensional chaotic mapping to generate a large number of random data points. A discrete fractional random transform (DFRNT) and Arnold transform (AT) are discussed in the intensity-hue-saturation (IHS) color space, and another image encryption scheme is presented in [2]. Then, each color space component is encrypted using individual methods. An example of a picture encryption approach proposed based on the Arnold and Gyrator transforms can be found in [3]. The multiple number of subimages is first separated into amplitude

and phase of the gyrator transform. Then, scrambling using Arnold transform takes place. The secret to these parameters would be the input key to the hiding method.

An FRFT-based image encryption for double or multiple pictures is previously proposed by Tao et al. [4]. The algorithm was also published in the Journal of Electrical and Computer Engineering. Finally, the different orders of IDFRFT of interpolated subimages were summed together to end up with the encrypted image. Together with the encrypted image, the generated secret keys to decrypt every subimage contains the whole transformation orders in the implemented FRFT.

In another application, Zunino [5] applies Peano-Hilbert curves to permute pixel positions in an image so that spatial autocorrelation in the image is suppressed. Zhang and Liu proposed the image encryption solution based on the skew-tent map system with the permutation-diffusion architecture in [6]. In this proposed scheme, the length of the P-box is made equal to the size of the original image; pixel placements are completely reorganized. The randomness of encryption and its security effect can be greatly improved with diffusion from the keystream in this stage, dependent upon the original picture and the key. Zhao and Chen [7] proposed ergodic matrices as a cryptosystem of digital photo scrambling. Ergodic matrices, their isomorphism, and the set of permutations were analyzed also by these authors. A new kind of permutation method was introduced by Zhu et al., which can change the value and position of the pixel such that it confuses and weakens a grayscale image at its bit level [8].

Then it applies logistic map to encrypt the already permuted image in addition to the use of Arnold cat map in permuting the bits of the picture. In this third class, chaotic sequences generated by chaotic system were used as encryption keys besides exploiting in Huang and Nien's [9] novel pixel shuffling method for colour picture encryption. The generalization to 3D of the two-dimensional chaotic cat map was first proposed in [10]—established in [13]—to yield a fast and safe symmetric picture encryption method. This combines both value and location randomization of the pixel in an image using the 3D cat map. Picture encryption technology was proposed by Wang et al. in which a simple Perceptron combined with a high dimensional chaotic

system is used to develop three types of pseudorandom sequences [11]. In addition, the weight of each perceptron neuron and a set of input signals are generated based on a nonlinear process. A new proposal for picture encryption technology contains the combination of diffusion and permutation processes and was proposed by Wang et al. lately [12].

After the original figure is segmented into blocks, a spatiotemporal chaotic system is used to generate the pseudorandom sequence in order to rearrange and spread the blocks. Picture encryption security has drawn a great deal of research interest. Almost all permutation-based encryption schemes with high redundancy have been found insecure against a ciphertext-only and known/chosen-plaintext attack. This is hardly surprising since the secret permutations can be recovered in a simple manner by using plaintexts compared to permuted ciphertexts; its compute cost is high.

Besides, cryptosystems are integer-based domain while chaos systems are continuous. The significant limitations of one-dimensional chaotic cryptosystem are small space and inadequate security [1, 13]. In the present work, we introduce a new picture encryption technique based on Rubik's cube idea. First, the Rubik's cube principle is applied to shuffle the pixels of the original grayscale image, where only the position changes. Suppose we need to do a bitwise XOR with the odd rows and columns to some randomly generated secret keys. Then, using the same secret keys but reversed, we do a bitwise XOR with even rows and columns. These can be run for repeated numbers of times until the maximum number of iterations is achieved. The suggestion for the encryption algorithm is numerically tested to secure and maintain validity in this research. For instance, technology has been developing tremendously over years but also has some dark sides too.

One of them is illegal duplication of digital intellectual property. Many efforts have been made to address this problem. Mainly, the ones that are done are encryption-based primary ones. The main purpose here is to implement the encryption of digital photos. The process of translation of data into some unreadable mode by some sort of algorithms is what we refer to as encryption, and it is also a method whereby access to

only the allowed people takes place, or in other words, authentic users. Most of the time, the main purpose of being carried out is the encryption of digital photos. Although there are now popular data encryption techniques, comprising symmetric key algorithms, asymmetric key algorithms, and algorithms that take into consideration elliptic curve cryptography, they do not represent the best for picture encryption basically because these ones are more useful from moment to moment communication or when matters request instant data encryption. Pixel position permutation, value transformation, and chaotic systems are the three main categories into which the proposed encryption methods of recent years can be classified. Besides, most of the work has been done in image encryption. Already it is found that some permutation-based encryption systems are attackable by attacks such as chosen-plaintext and ciphertext alone. It is logical because such methods have a high degree of data redundancy and because plaintext and ciphertext comparisons can be used for redeeming secret permutations.

1.2 Background

The demand for safe data transfer has increased due to the quick growth of technology, which has sparked the creation of sophisticated encryption methods. Inspired by the well-known problem, the Rubik's Cube algorithm offers a novel method of protecting coloured pictures. With rotations like to those on a Rubik's Cube, this technique rearranges picture pixels, making unauthorised decryption exceedingly difficult in the absence of the right sequence. The algorithm's strength and adaptability have been demonstrated by earlier studies, which also included successful mobile implementations and improvements made possible by integrating it with other cryptographic methods like the RC6 algorithm. This multi-layered method makes encryption more difficult and safe, which makes it appropriate for real-time applications that need to send data quickly and securely. The current work seeks to make a substantial contribution to the field of data security and encryption technologies (Zenodo, IJEAT, OUCI, CiteFactor) by utilising these cutting-edge methodologies.

1.3 Cryptography

One of the most popular techniques for protecting the privacy of communications between parties is cryptography. Using a shared key that is encrypted across an unsecure channel, this approach turns text into ciphertext. The ciphertext may be decrypted back to the original plaintext using a working key. Without the key, no one can access the plaintext. Numerous elements need for safe communication across unprotected networks, such as B: confidentiality key exchange, authentication, non-repudiation, and data protection. Fig. 1 shows the cryptosystem in graphic form.

Generally speaking, there are two kinds of cryptography used to secure data. To accomplish this, hash functions, private-key cryptography, and public-key cryptography are often employed strategies. The kind and length of keys used determine the type of encryption algorithm. The data is cypher text, as shown in the provided figure, and is sent to the recipient via encryption and decryption. When sending data to a recipient, the sender attempts to encrypt the data or information into a cypher text first. The sender also possesses keys, which the recipient may use to decode the data and obtain the data that was provided.

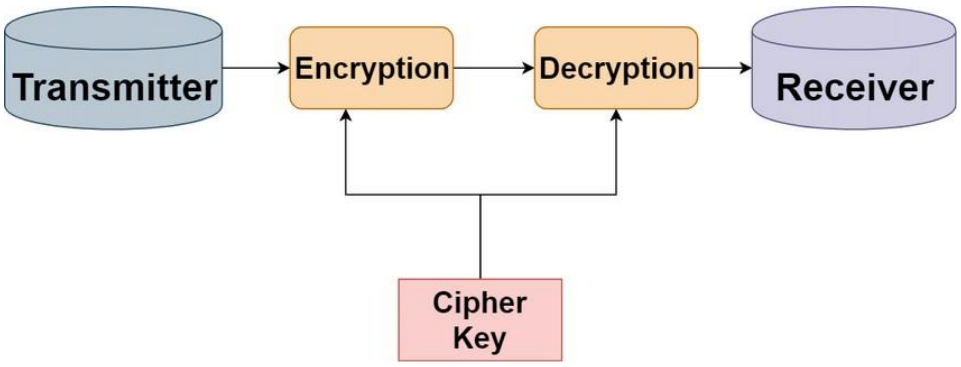


Figure 1.3.1: Representation of encryption-decryption algorithm

1.3.1 Symmetric / Secret Key Cryptography

Acknowledged also as single-key, shared-key, symmetric-key, and secret-key cryptography. To encrypt and decode private data, private key technology is employed. Using the sender's key, the original data, or plaintext, is encrypted. With a comparable key, the recipient decrypts the communication and retrieves her plain text. Only individuals who are authorised to encrypt or decode data know the key. Nevertheless, key distribution is an issue even if this method offers strong transmission security. Your complete data can be easily obtained if someone were to steal or break into your key.

In other words, a symmetric key is a type of cryptography where data or information is encrypted and decrypted using one key, or the same key. The key must be securely exchanged between the sender and the recipient. It can handle higher encryption volumes and is quicker than asymmetric key cryptography. Popular symmetric/secret key encryption techniques include DES (Data Encryption Standard), 3DES, and AES (Advance Encryption Standard). It is mostly used in scenarios like storage, database encryption, and secure communication when data has to be encrypted and decrypted.

1.3.2 Asymmetric / Public Key Cryptography

This method is also known as an asymmetric or public key cryptosystem at times. For both data encryption, two independently utilised, mathematically linked keys are used. as well as decoding. Using this strategy, it is difficult to locate the other key or read its contents once a private key has been used. The technology must be operated using all keys. The decryption key is kept private and is referred to as the private key, whereas the encryption key is kept openly and is known as the public key.

To put it another way, an asymmetric key cryptosystem uses a public key and a private key. While the public key is available to everyone and is used to encrypt data, the private key is kept secret and is utilised to decode data. In this case, the messages are encrypted using the receiver's public key, and the only key required to decode them is

the receiver's private key. Most commonly, asymmetric key cryptosystems include a wide range of common algorithms, such as:

1. RSA (named after the developers Rivest, Shamir, and Adleman): The most widely used of public key cryptosystems; applies primarily to the protection of information; also used for preparing small blocks of data to be signed digitally.

2. ECC (Elliptic Curve Cryptography): That is arithmetic over elliptic field curves over finite fields. It's more secure than RSA, yet with smaller key sizes.

3. DSA: Digital signature generation for the authentication and enforcement of the integrity of data with the application of encryption and decryption.

4. Diffie-Hellman: This technique allows two persons to safely exchange a secret key over an unprotected connection; it is not directly used to encrypt or decode data or information. Symmetric encryption can then be performed using the shared key. This method outperforms most others in terms of speed when it comes to encrypting huge amounts of data.

5. EIGamal: This method, which is used for digital signatures and encryption, is entirely based on Diffie-Hellman. It protects the privacy of information or data.

Characteristic	Symmetric Cryptography	Asymmetric Cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plaintext size	More than the original plaintext size
Known keys	Both parties should know the key in symmetric key encryption	One of the keys is known by the two parties in public key encryption
Usage	Confidentiality	Confidentiality, Digital signature

Table 1: Difference Between Symmetric and Asymmetric Cryptography

1.4 Steganography

It is referred to as the science of surreptitiously transmitting data via purportedly trustworthy carriers in order to conceal its existence. It doesn't even know the message exists as a result. The user would not be aware that a cover containing data exists and would not attempt to comprehend it when he saw one. By applying a certain algorithm, a Stego system encoder may inject sensitive data into cover media. A hidden message might be an image, ciphertext, bitstream of plaintext, or any other kind of data. The covered object is called a stego object once the hidden data has been inserted. To obtain the original information, the decoder system employs the same stego technique to select the appropriate channel for stegoing the stego object. It is also received by the recipient. because the sender wanted to forward it.

Steganography is a method used to hide data from being found in ordinary files or messages. Text documents, audio files, video files, and image files may all include secure data. Steganography's primary objective is to protect the secret message, which is only visible to the sender and receiver.

Techniques for steganography might be as basic as writing to an unseen file inside another file or as sophisticated as encrypting picture or video data. To prevent involvement from other third parties, it offers an extra layer of encryption for data or information. In a variety of contexts, including military and interpersonal communication, it is frequently utilised for secure communication and information security.

To ensure that our data is securely and conveniently transferred to the recipient, for instance, a secret message or data is concealed in the picture, audio, and video files. This distinguishes it from encryption, which gathers a message and renders it unreadable or writeable but leaves the message's existence visible. Steganography, in its broadest sense, is a technique that involves concealing a secret message on the cover of media or files. The concept is to use suspensions to stop secret data from being shared. Steganography comes in three forms: audio, video, and picture. The technique of hiding files, messages, photos, audio, or video within another file, message, image, or audio or video is known as steganography. We'll remove it at its destination later. It

comes from the Greek terms graphia, which means writing, and stegano, which means covered or hidden.

Although steganography and cryptography are not the same, their combined use can increase the security of information that is protected and hinder the discovery of covert communication. Basically, the goal of steganography is to conceal the existence of data or information, while the goal of cryptography is to render the data unreadable. The user would not be aware that a cover containing data exists and would not attempt to comprehend it when he saw one. By applying a certain algorithm, a Stego system encoder may inject sensitive data into cover media. A hidden message might be an image, ciphertext, bitstream of plaintext, or any other kind of data. Steganography comes in several forms, encompassing picture, audio, video, and text data.

1.4.1 Text Files

Text steganography is the word used to describe the method of encoding sensitive information into text. Text steganography requires very little memory because this file type can only hold text data. It makes it possible for senders and recipients to communicate or exchange files quickly. Text steganography is the process of hiding data or information behind text. Let's use an example to better understand. Let's say you have to convey the hello message using text steganography. In such case, you may write it as a poem or as a full text message, with H standing for "hope you are doing well today," e for "everything is good," and y for "you are great.That is, text steganography is majorly considered the manner in which the data or some information has been hidden in the plain text in such a manner that it runs through a channel of communication without any risk to the data. The aim of text steganography is to secretly and almost imperceptibly transfer information.

1.4.2 Image Files

This method involves adding data to a picture's pixel structure so that alterations to the cover image are invisible to an attacker. LSB method is a popular approach for picture steganography. picture steganography is the process of hiding data or information behind picture files. Several methods are employed in image steganography, including:

1. The Least Significant Bit (LSB) method is a crucial one for picture steganography. It encodes secret information or data by modifying the last bits of particular pixels in a picture.

2. Masking and Filtering: This picture steganography technique is crucial. It modifies the information or data to a watermark pattern. It is quite tough to find and eliminate this strategy.

3.Redundancy-Based Techniques: One crucial method for image steganography is this one. It converts the confidential data or information into an unnecessary colour scheme. This technique is incredibly safe and hard to find and uninstall.

The methods mentioned above are excellent for steganography of images. All of these techniques are used to actual issues to effectively safeguard data or information.

1.4.3 Audio Files

This is how voice information is concealed. There are several ways that confidential information might be concealed in audio recordings. Think about phase coding. The data or information is transformed into an audio or recorded form in this steganography. The technology of audio steganography holds great importance in data or information protection.

1.4.4 Video Files

It's a way to encrypt private information included in the frames of a video clip. Using this steganography technology, data or information is encrypted and converted into an image or video format to keep it safe from prying eyes. This makes the process ideal for steganography.

1.5 Cryptography vs Steganography

Based on several parameters, Table 2 shows how cryptography and steganography differ from one another. Definitions, targets, carriers, input files, keys, visibility, security services provided, attack types, attacks, consequences, and applications serve as the foundation for comparisons.

Criteria/Method	Steganography	Cryptography
Definition	Cover writing	Secret writing
Objective	Maintaining existence of a message secret ,Secret communication	Maintaining contents of a message secret ,Data protection
Carrier	Any digital media	Usually text based
Input file	At least two	One
Key	Optional	Necessary
Visibility	Never	Always
Security services offered	Authentication, Confidentiality, Identification	Confidentiality, Identification, Data Integrity and authentication Non- repudiation
Type of Attack	an aim of finding whether it is stego file or not	Cryptanalysis
Attacks	Broken when attacker reveals that steganography has been used. known as Steganaly- sis.	Broken when attacker can understand the secret message. known as Cryptanalysis
Result	Stego file	Ciphertext
Applications	Used for securing information against potential eavesdroppers	Used for securing information against potential eavesdroppers

Table 2: Differences Steganography and Cryptography

Steganography is used for cover writing, whereas cryptography is used for secret writing. This is the main distinction between the two types of writing. Transforming plain text into cypher text is known as cryptography, and it is used to prevent other parties from discovering the true facts or information. The data is transformed into several formats, including text, video, picture, and audio files, throughout the steganography process.

Steganography is used to protect data or information against prospective eavesdroppers, whereas cryptography is used to secure information from them. Cryptography is one of the most widely used methods to ensure the confidentiality of communications between parties. A key that is shared, used to encipher, and ciphered across an unsecure channel enciphers text to a ciphered text. The ciphered text can be deciphered back to the plain text with the use of a working key. Steganography is the act of hiding data in plain sight so that it cannot be found inside routine files or messages. Text data could be secured inside text documents, audio records, picture files, or video. In other words, it could be said that the main purpose of steganography is to protect a secret message, which is fully invisible to all but the sender and receiver.

1.6 Rubik's Cube Principle

The concept of image encryption using a Rubik's Cube is this itself. In fact, the ability to come with really simple operations at a high level of permutations of the cube is used here so that the level of security in the encryption process is enhanced. Some such applications are discussed below:

1.6.1 Concept of Rubik's Cube Principle

- The concept of a picture as a three-dimensional array of pixels is employed in this analogy, just as the Rubik's Cube is a three-dimensional array of coloured tiles. This makes it possible to apply 3D transformations to the picture data.

- Block & Permutations: In this kind of encryption, the image is split into small blocks or sub-images, in the manner that is evident in workings of a Rubik's Cube. Under a secret key, the permutation operates to rearrange or permute the positions of these blocks, which is the first implementation on the encryption process. That's because the process changes the position of blocks.

- Rotational Operations: Within a block, pixel rows and columns may be cyclically displaced or rotated with each other. This is analogous to the rotation

of Rubik's cube faces. These rotations can, obviously, be largely controlled by extra keys. The security level is increased with these rotations, and the complexity of the image structure also increases

- Numerous Transformation Rounds: Block permutation and pixel rotation can be done numerous times to boost security. An attacker will find it more challenging to undo the operation without knowing the precise order of transformations and the keys used in each round as the complexity increases.

1.6.2 Steps in Applying the Rubik's Cube Principle

- Partitioning: A non-overlapping block of equal size is made on the image. A M×N size of an image, for instance, could be partitioned into the size of blocks M× N.

- First permutation: Blocks are permuted with a secret key. According to that key, blocks get new locations. So a picture is decrypted only with the same key.

- Row and Column Shifts: The shifts of rows and columns are circular, so that goes to move from the bottom to the top etc. by the use of the other key. For example, a row shift may be implemented as circularly shifting the row by N places in the right direction by N places in the right direction.

- XOR Operation: Here, after shifting, the pixel values within the block are XORed with the key matrix. In fact, generally, it is for the purpose of modification of the pixel value with the key matrix; instead of the XOR operation, it is another kind of layer of encryption.

- Repetition: Basic repetition of permutation, shifting, and XOR operations improves security. In every new round, a new set of key is

derived, which makes complexity higher for the decryption of the encryption algorithm.

1.6.3 Advantages of Using the Rubik's Cube Principle

- High Security: A very secure encryption method that is impervious to popular assaults including brute force, differential, and statistical attacks is created by combining block permutation, pixel shifting, and XOR operations.
- Complexity and Unpredictability: Unauthorised parties will find it very challenging to decode the picture without the right keys because to the several layers of transformations and the usage of secret keys, which add a high degree of complexity and unpredictability.
- Efficiency: The encryption is appropriate for real-time applications since the related operations (shifts and permutations) are computationally efficient and simple to perform in hardware or software.

CHAPTER 2

LITERATURE REVIEW

Increased security is possible to be achieved with random phase encoding-based picture encryption techniques in gyrator domains by the observation of iterative structures with added random phases. Two-dimensional chaotic mapping, based on the expressions serving as encryption keys and initial values, are built to them. Consequentially, provided relations for a chaotic mapping can serve as strong substitutes of traditional algorithms and secure storing and sharing based on symmetry. Besides, the angle parameter of the gyrator transform works as an added key and makes this algorithm even more secure. Considering these chaotic maps as joint keys and the parameters of the gyrator transform, numerical simulations lead to the discovery that the encryption scheme works successfully in secure encryption of pictures.[1]

The proposed colour image encryption method explores the intensity-hue-saturation (IHS) colour space, discrete fractional random transform (DFRNT) and Arnold transform (AT) combination. It has been observed that DFRNT is a suitable scheme for encrypting the intensity component using pixel value obfuscation from its position and that AT shuffles the hue and saturation components. The technique ensures approximately equal security and is also more storage effective than traditional double-random-phase encoding methods. Further improvement involves the encryption keys for the DFRNT's random matrix and fractional order into which the Arnold transform can undergo a number of iterations. Numerical simulations confirm the feasibility and effectiveness of the strategy with performance studies against different attackers and scenarios.[2]

Unlike the available methods based on single order of FRFT, the proposed scheme is utilizing multiorders for encryption of images and, thus, security is enhanced by increasing the key space. Encryption is accomplished by addition of inverse

discrete Fourier transform of multiple orders of interpolated sub-images and decryption uses a obtained linear system derived in fractional Fourier domain analysis. This technique enables double or more image encryptions using the FRFT orders as secret keys; hence, retaining computational efficiency with the fast-Fourier-transform-based methodology. The quoted experimental results showed the high sensitivity of decryption to changes in the transform order, and this ensures the robustness of the technique. [4]

The research was thus conducted on a communication system with several mobile devices with imaging sensors, a server, and the Rubik's Cube encryption technique to investigate the efficiency and suitability of using the said technique to protect image transfers. More so, the transfer of images cannot go without their encryption. This is because it ensures the images are saved from third-party views. The application demonstrates the effectiveness of the Rubik's Cube algorithm on mobile devices and has a secure manner in the place of encrypting and decrypting images. The analysis shows the dependability and adequacy of the algorithms under dynamic settings, hence affirming that device-to-server communication should be both safe and dependable.[5]

The proposed image cryptosystem furthers the security of the iris-based systems against replay attacks by the use of diffusion and permutation operations. In this, a cover image has been divided into the blocks, and then all blocks are subjected to the concept of Rubik's cube after being permuted using a permutation key for scrambling. Then pixel values are modified using XOR to get a resultant encrypted picture. It has been experimentally tested over the CASIA database iris photos and connoted that the system is immune to statistical, differential, and exhaustive attacks. In this regard, it attains an elevated security rating, as all the results were pointing to the cryptosystem being reliable and effective in its protection against the commonest security threats.[6]

This new encryption system, based on the 3-D Rubik's cube principle, combines the RC6 algorithm to protect a set of pictures in a most secure way. Firstly, the principle of diffusion is introduced when the pictures are separately encrypted

using RC6. These RC6-encrypted pictures form the faces of the 3D Rubik's cube, which is given another level of permutation by encryption. The result of the simulation concludes that this approach is reliable, robust, and secure. Finally, the encrypted pictures are efficiently decrypted at the receiver end by using a wireless OFDM method. The efficiency of the method is established by the outstanding results obtained from the quality evaluation of the encrypted images at the receiver end [8].

The proposed Rubik's cube and XOR-based encryption algorithm, called CIERPF, improves plain image sensitivity and completely avoids plain image-related attacks by injecting dynamic initial random value generation along with Henon map vectors for key sequence derivation, they append to the abstract. In addition, it offers prime factorization for diffusion and dynamically changing random seeds with key generation, making it a very strong defense against differential attacks. Effectiveness against differential cryptanalysis was achieved through different simulations, showing strong key space, sensitivity, and uniformity in the distribution of the pixels of a cipher picture. All in all, CIERPF is proving quite promising for safe transfer of multimedia over untrusted networks; hence, it provides a viable encryption method for defense against sensitive picture data. [10]

According to them, the RubiCrypt method employs a Rubik's cube arrangement as a multiple-dimensional security key to encrypt pictures. It effectively mixes the input pictures by making use of all the 43 quintillions of possible configurations of the cube. The use of OpenCV imaging processing techniques has encryption and decryption with real-time cube scanning. The analysis and the testing results show that the encryption strength of RubiCrypt is high and hardly affected by statistical and differential attacks, considering the quality of encryption, which is superior, and important picture data concealment, which is greatly enhanced. As a result, it has great potential for safe image transmission and storage in settings where security is greatly concerned.[12]

Based on the abstract of this, the published article has been aimed at the imperfectness of the already existing techniques, either lacking security or being inefficient, hence aimed at developing a method that will provide him with a technique of encryption and decryption of digital color pictures that he can trust and is efficient in his usage. He intends to maintain it computationally efficient but at a high level of security because, for this approach, there is a compulsion that it should be largely used for electronic mail and internet communications. To validate its effectiveness, the research is associated with extensive testing followed by deployment to compare performance measures against alternative techniques of encryption. The results would not only reflect the level of measurement but also confirm the technique as a reliable method for the secured transfer and storage of color digital photographs in indigenous digital environments.[13]

Abstract: In the following work, the block-cipher algorithms RC6, Twofish, and Rijndael have been thoroughly analyzed for their performances. Emphasis has been placed on the execution time more than the measures of resource utilization. These algorithms were designed for the AES competition; they have flexible block and key sizes to fit different security requirement values. Rijndael and Twofish have uniform encryption and decryption structures, and RC6 offers a different method. Key sizes have been tested at 128, 192, and 256 bits to offer an indication of the operation of algorithms across several settings, given that this is information that must be collected to determine which cryptographic applications are best to be implemented. [14]

From the abstract, the article investigates an implementation of picture security based on ideas of Rubik's cube, using XOR and pixel scrambling for encryption and decoding. This betterment in data security is contrary to the fast development of technology and at the same time provides a strong safeguard for photos that are regularly sent through various channels. A wide-ranging testing with every type of image is undertaken to validate the effectiveness of the algorithm, and the results obtained indicate that it can be effectively used for data integrity and

confidentiality. By employing mechanics from Rubik's cube-inspired strategies, the method is built on a safe and high-performance infrastructure to increase picture file security in modern digital communication environments.[16]

Abstract: This paper introduces 512-bit RC6, a new secret-key block cipher improving on the legacy 128-bit RC6 but this time aiming at better speed and security for the Advanced Encryption Standard (AES). Doubling the previous RC6 to 256 bits, this new development, by adding a Feistel network iterated 20 times, offers very strong encryption capabilities. The technique generates a considerably larger Avalanche Effect when compared to its predecessor. It shows higher sensitivity to alterations in either the plaintext or the key. Larger Block Size: 512 bits, used, act well in enhancing the increased security and at the same time addresses dictionary and matching attacks most effectively. Hence, this is a great step toward security and efficiency in cryptanalysis compared with the original 128-bit RC6. [17]

Per the abstract, this article talks about a new technique of encryption for color images by using the Intensity Hue Saturation (IHS) color space, using Discrete Fractional Transform, and Arnold Transform. The proposed technique shows better results in terms of security since the hue and saturation components are scrambled using Arnold Transform, where the intensity component of encryption shows the use of DFRNT to achieve pixel value as well as location secrecy. DFRNT, despite its equivalence in security to techniques like double-random-phase encoding, reduces the storage requirements for encryption keys. To enhance the security of the proposed model against known-plaintext attacks, noise and occlusions, encryption parameters such as fractional order of DFRNT, the specifications of the random matrix, and the number of iterations of Arnold transform were considered. Numerical simulations confirmed the feasibility and effectiveness of the method to ensure protection of color images.[19]

An optical image encryption scheme based on Gyrator and Arnold Transforms is presented in this paper, guided by the following abstract. An algorithmic partition of the input to the gyrator transform into subimages in amplitude and phase is

achieved. Scrambling with Arnold Transform of each subimage formed by the GT is further carried out for increased security. The gyrator transform is a recursive over the random spectrum of these scrambled subimages, hence offering advantages of more robustness to the encryption. The keys are the parameters controlling the separation in sub-images and the gyrator operation that would secure the algorithm. Numerical simulation supports that it is feasible to carry out the encryption procedure on an electrooptical setup and demonstrates the security and efficiency of the proposed algorithms in optical image encryption applications. In addition, it would be more secure against known/chosen-plaintext attacks.[23]

Abstract This paper introduces a new multi-order picture encryption scheme based on fractional Fourier Transforms (FRFT). In this, adding inverse discrete FRFTs of interpolated sub-images at different orders will give the encrypted picture. As a result, high security is achieved against possible decryption without the proper transform orders. In relation to existing system that are based on FRFT, the proposed system has large key space, and it supports multiple picture encryption; thus, it is more secure. This is crucial in ensuring that the computational efficiency of the algorithm is maintained, being characteristic of the fast Fourier transform-based methods. It has been validated experimentally, and the encryption is effective and reliable for the protection of digital images while demonstrating the high sensitivity of image decryption to transform order variations[25].

The abstract presents a chaos-based scheme of picture encryption using the logistic map for diffusion and bit-level permutation using the Arnold cat map. Many simulation runs were made to endorse the dependability of effectiveness of the system, and it high encrypts digital photos. The proposed cryptosystem combines the extra security features by introducing chaotic maps that help control the undesired access and data integrity in storage and transmission. In brief, this work enhances digital picture encryption techniques using the theory of chaos under recent threats. [27]

CHAPTER 3

METHODOLOGY

3.1 Methodology for Encryption:

This methodology encrypts a grayscale image using a process similar to scrambling a Rubik's cube. The steps are detailed below:

Initial Setup

1. Image Matrix: The image is represented as a matrix I0 of pixel values with dimensions M*N.
2. Random Vectors: Create two random vectors, KR and KC, with lengths M and N respectively. The values in these vectors must be greater than 0 and less than 2A(where A is a constant). KR and KC should not have constant values.
3. Iterations: Set the maximum number of iterations, ITERmax, and initialize the iteration counter ITER to 0.

Iterative Process

4. Increment Counter: Increase the iteration counter by 1:

ITER=ITER+1.

Row Operations

For Each Row i in I0:

5. Calculate Row Sum**:** Sum all elements in the row to get A(i).
6. Modulo Operation: Compute MA(i) as A(i) Mod 2.
7. Circular Shift**:** Depending on MA(i):
    - If MA(i)=0 : Right circular shift the row by KR(i) positions.
    - Else: Left circular shift the row by KR(i) positions.
    - Apply XOR and bitwise rotations to the row elements.

Column Operations

For Each Column j in I0:

8. Calculate Column Sum: Sum all elements in the column to get B(j).
9. Modulo Operation: Compute MB(j) as B(j) Mod 2.

10. Circular Shift: Depending on MB(j):

- If MB(j)=0: Upward circular shift the column by KC(j) positions.
- Else: Downward circular shift the column by KC(j) positions.
- Apply XOR and bitwise rotations to the column elements.

Final Steps

11. XOR Operation Rows**:** Using KC, perform XOR operations on each row of the scrambled image.
12. XOR Operation on Column: Using KR perform XOR operations on each column of the image.
13. Check Iterations: If ITER equals ITERmax, the encryption process is complete, and the encrypted image IENC is obtained. If not, repeat from step 4.

Secret Keys

- KR: Random vector for rows.
- KC: Random vector for columns.
- ITERmax: Maximum number of iterations.
- Circular Shifts: Moving elements in the row or column circularly to the left or right.
- XOR Opeartion: A bitwise operation that combines pixels with elements from vectors KR and KC.

By following these steps, the pixel values in the image are scrambled multiple times, making the image encrypted.

3.2 Methodology for Decryption:

It decrypts a ciphertext image (IENC) using a secret key (KR,KC) maximum number of iterations (ITERmax). Here's a step-by-step breakdown of how it works:

Initialization

1. Counter Setup: Set the iteration counter ITER = 0.

Iteration Loop

2. Increase the Counter: Counter is incremented by one, so it is now ITER + 1.

3. Bitwise XOR operation :XOR operation on columns: Perform an exclusive XOR of the KR vector with each of the columns of the encrypted image.

4. Sum Over Each Column: Assume a column j of the permuted image (ISCR). Sum all elements in a given column, denoted by BSCR(j).

5.Modulo Operation: Modulo-2 addition of sum BSCR(j).

CircularShift: If MBSCR(j) is set, this will perform a circular shift of the column j by KC(i) positions to the top; otherwise, the bit string will be shifted downward.

6. Row Operations: Summing of Each Row: For every row i of the IRSC image calculate the sum of all pixel values of that row and denote it by ARSC(i).

Modulo-2 Operation: Compute modulo-2 sum of the addend ASCR(j) and store in MASCR(j). Circular Shift: All row elements are cyclically shifted left (or right)most by K(i) positions in the direction indicated by the binary value of the MASCR(j) of the control word.

3.3 Implementation

3.3.1 Encryption

In order to encrypt the picture, we must preserve the photos in the "input" folder. The code uses the PIL package to take in a picture, turns it into RGB matrices, and then uses the Rubik's cube technique to begin the encryption process.

After that, the encrypted photos are kept in a different folder. The values of Kr, Kc, and Iterations (ITER_MAX) are kept in a file called "keys" following encryption.

3.3.2 Decryption

This code begins the decryption process given the encrypted picture and the Kr, Kc, Iterations (ITER_MAX) variables.

3.3.3 Data Set Used

Since this project focuses on encryption algorithms, any type of picture may be used as input to create an output that is highly secured and safe. We use common black and white pictures, such Lena, Black, Baboon, and Checkerboard, to assess the outcomes. The following academic article describes the Rubik's cube concept, which is the basis for the picture encryption technique that our project executes. Chouinard, J. Y., Loukhaoukha, K., and Bernardai, A. (2012). a technique for safe picture encryption based on the Rubik's cube theory. Electrical and Computer Engineering Journal, 2012, 7

The usage of the algorithm for black and white photographs is described in the publication from which we are implementing the encryption method. We expand on this encryption technique to support RGB (colour) pictures.

CHAPTER 4

RESULTS AND DISCUSSION

Two randomly generated vectors are used to shuffle the original picture's pixels in a manner akin to a Rubik's cube in order to produce the encrypted image. Subsequently, bitwise operations are carried out row-wise and column-wise using the same vectors. To lessen the link between the encrypted and original pictures, an XOR operation is used with a key to odd columns and rows in the image. The same key is turned, and even columns and rows of the picture are subjected to an XOR operation.

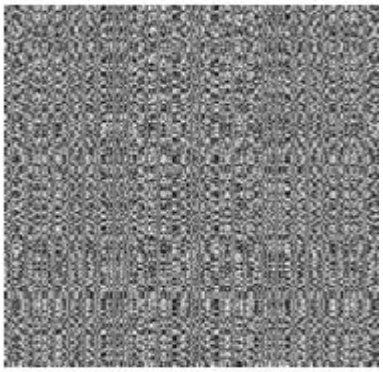
Safe picture cryptography should be resilient to a variety of attacks, including brute-force, applied arithmetic analysis, plain text, and cipher-text-only assaults. In our primary reference work, a thorough security study of the proposed algorithm is carried out along with an applied math analysis and a safety evaluation on important areas. In addition, the technique was put through a number of tests to see how well it performed in terms of achieved encryption. One type of testing is visual testing, which compares and calculates the results for the united average changing intensity (UACI) and number of pixels change rate (NCPR).

The encrypted image's pixel grayscale values differ from the original pictures' pixel grayscale values, as demonstrated by the UACI values. This makes it challenging to distinguish between picture pixels that are encrypted and original. Elevated NPCR % readings indicate that random pixel position changes have occurred. That means that high NPCR values and around 33% UACI values are necessary for an effective picture encryption scheme. The algorithm is satisfied with the proper values that were achieved during testing. According to the testing findings published in the study, the suggested method is capable of withstanding statistical, exhaustive, and differential assaults in addition to meeting high encryption requirements and having flawless concealment capabilities.

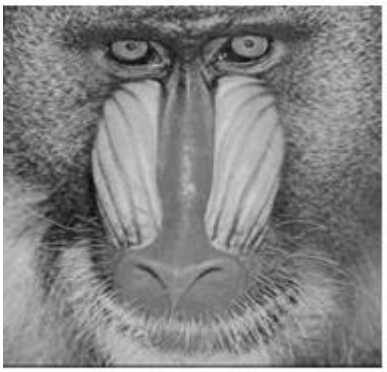
(a) Lena (original)

(b) Lena (encrypted)

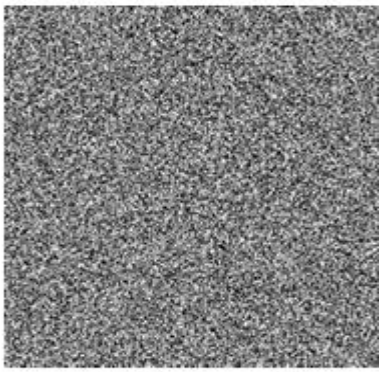
(c) Black (original)



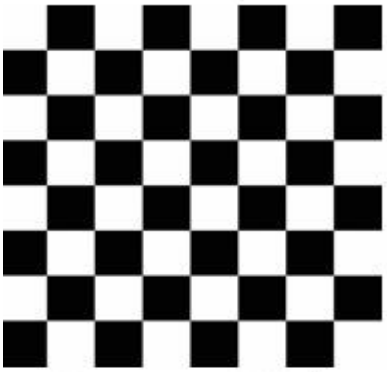
(d) Black (encrypted)



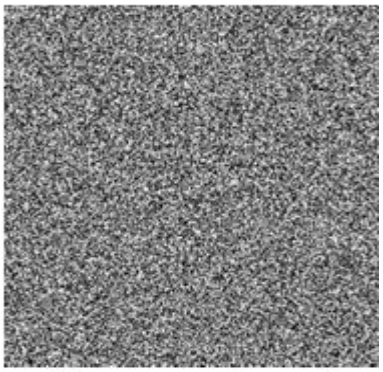
(e) Baboon (original)



(f) Baboon (encrypted)



(g) Checkerboard (original)



(h) Checkerboard (encrypted)

Figure 4.1 Original and Encrypted Image

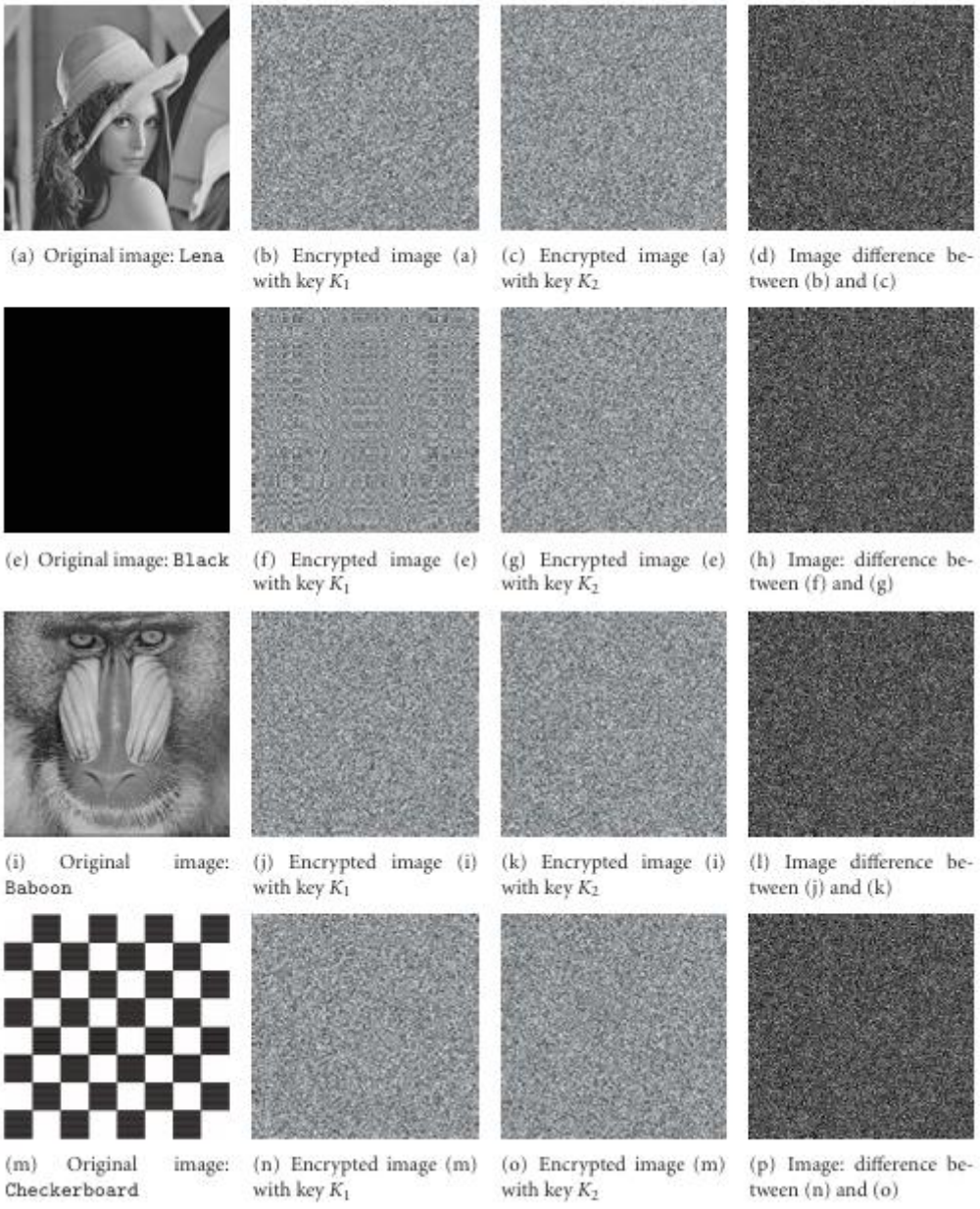


Figure 4.2 Key sensibility for image encryption using the proposed algorithm.

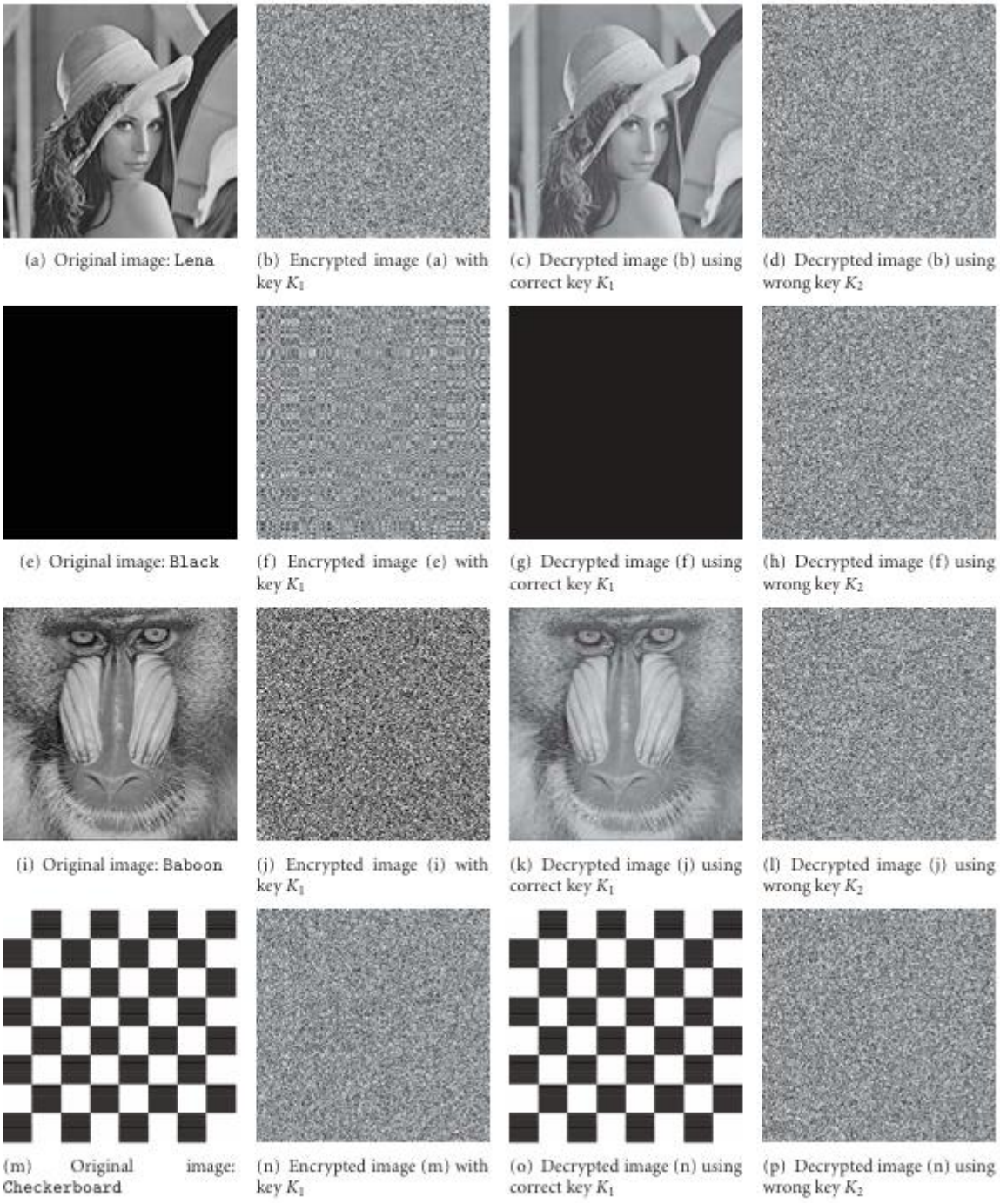


Figure 4.3 Key sensibility for image decryption using the proposed algorithm.

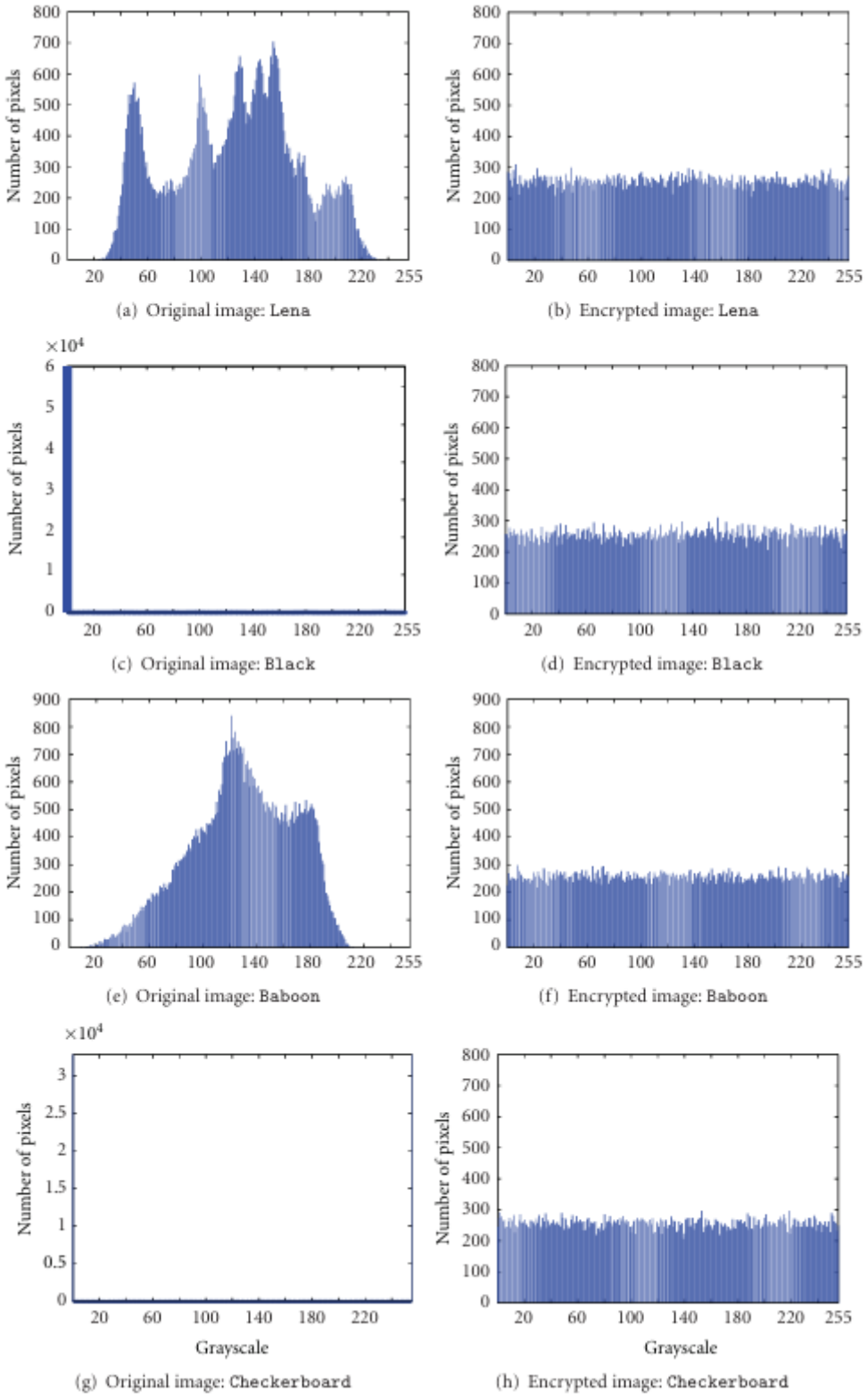


Figure 4.4 Histograms of original and encrypted images.

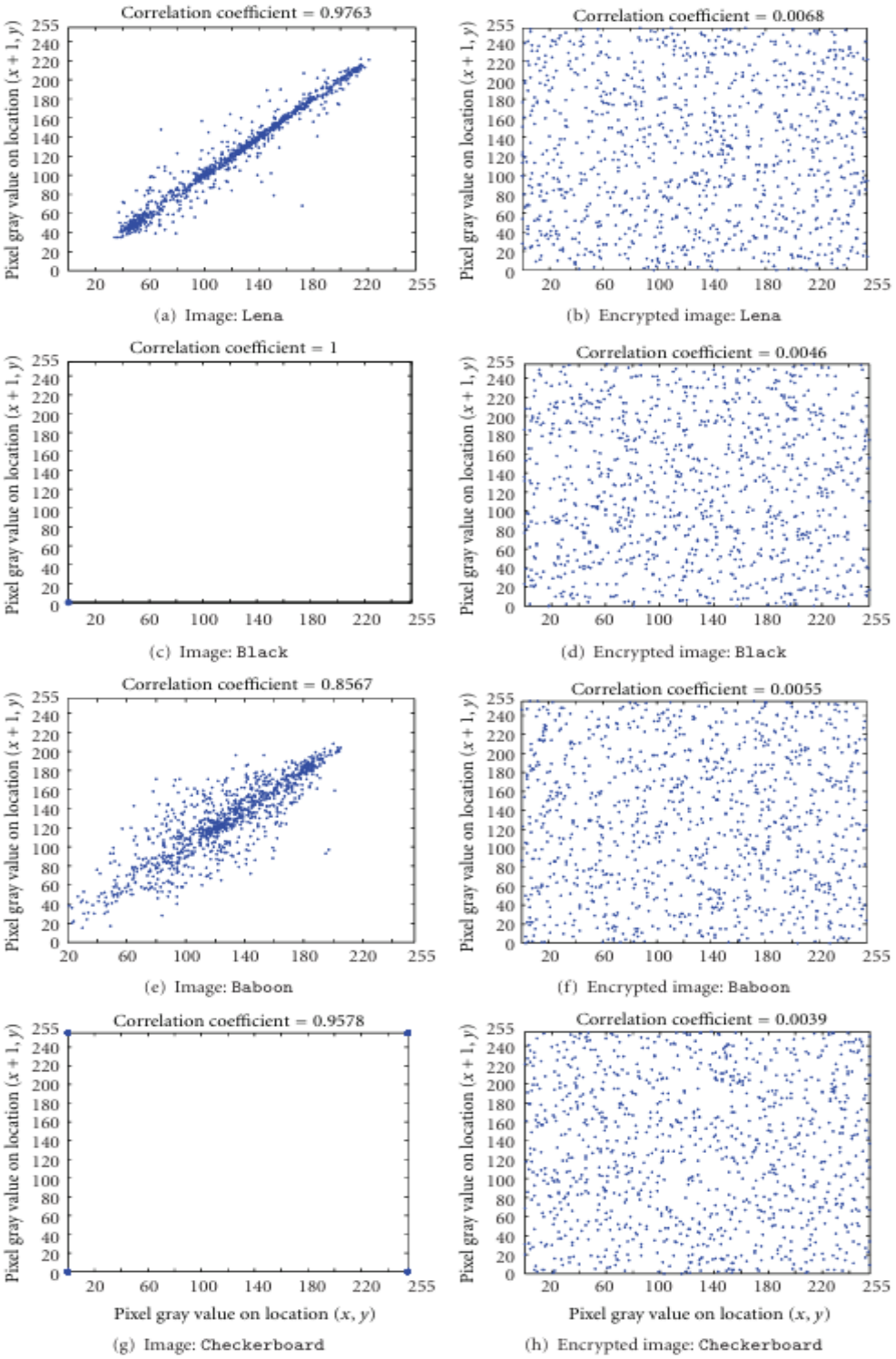
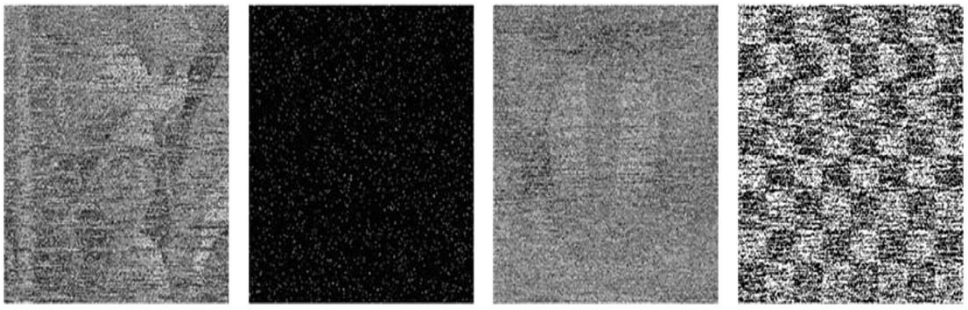
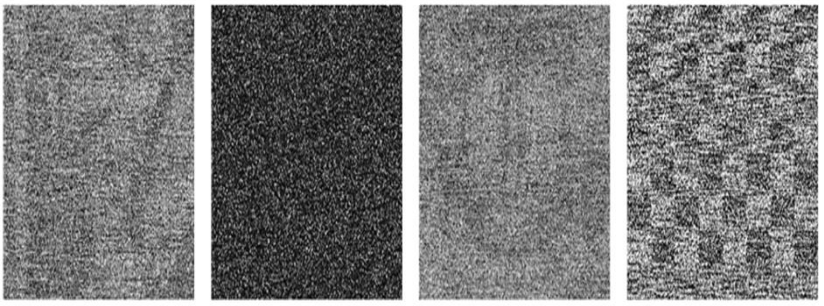


Figure 4.5 Correlation distribution of the pairs horizontal to adjacent pixels.



(a) Decrypted image: Lena (b) Decrypted image: Black (c) Decrypted image: Baboon (d) Decrypted image: Checkerboard

Figure 4.6 Attack by salt & pepper noise.



(a) Decrypted image: Lena (b) Decrypted image: Black (c) Decrypted image: Baboon (d) Decrypted image: Checkerboard

Figure 4.7 Attack by speckle noise

CHAPTER 5

CONCLUSION

This dissertation presents a novel and robust image encryption scheme based on the pixel evolvement principles of Rubik's Cube. This method is of high security and good for both Internet real-time protection and for evaluation because it was tested thoroughly and survived a variety of analytical, parametric assaults. Another novel study is in color image encryption in the IHS color space, using the discrete fractional random transform and Arnold transform. This scheme utilizes randomness in the use of the random matrix and fractional orders within the transform kernel for independent encryption of IHS components with joint encryption of pixel location and values to improve the level of security. This decryption technique is strong and accurate; it can be latched digitally with a small amount of storage that should be allocated for encryption keys. In security enhancement of the iris biometric systems against replay attacks, a good technique used for iris image encryption through block permutation as well as the cube principle of Rubik has been designed. Here, the technique proposed is a technique that divides the secret image into blocks and performs random permutations, circular shifts, and XOR operations to highly secure the encrypted image. The results of these experiments show that the cryptosystem resists well against statistical, differential, and exhaustive assaults from the statistical and entropy analyses, indicating it is a high security level.

REFERENCES

[1] Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. Journal of Electrical and Computer Engineering, 2012, 7.

[2] Ionescu, V. M., & Diaconu, A. V. (2015, June). Rubik's cube principle based image encryption algorithm implementation on mobile devices. In 2015 the 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. P -31). IEEE.

[3] Loukhaoukha, K., Nabti, M., & Zebbiche, K. (2013, May). An efficient image encryption algorithm based on blocks permutation and Rubik's cube principle for iris images. In 2013 8th International Workshop on Systems, Signal Processing and their Applications (WoSSPA) (pp. 267- 272). IEEE.

[4] Gomathi, T., & Shivakumar, B. L. (2015). Multistage Image Encryption using Rubik's Cube for Secured Image Transmission. International Journal of Advanced Research in Computer Science, 6(6).

[5] Helmy, M., El-Rabaie, E. S. M., Eldokany, I. M., & El-Samie, F. E. A. (2017). 3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm. 3D Research, 8(4), 38.

[6] Abitha, K. A., & Bharathan, P. K. (2016). Secure Communication Based on Rubik's Cube Algorithm and Chaotic Baker Map. ProcediaTechnology,24,782,7

[7] R.Vindhya & M.Brindha (2020). A chaos based image encryption algorithm using Rubik's cube and prime factorization process (CIERPF). Journal of King Saud University - Computer and Information Sciences

[8] Joffin Joy & Litty Koshy(2019). RubiCrypt: Image Scrambling Encryption System Based on Rubik's Cube Configuration.IEEE

[9] M. J. Aqel, Z. AlQadi, A. A. Abdullah (2018).RGB Color Image Encryption Decryption Using Image Segmentation and Matrix Multiplication.International Journal of Engineering and Technology, Vol. 7, No. 3.13, pp. 104-107, 2018

[10] Majed O. Al-Dwairi, Amjad Y. Hendi & Ziad A. AlQadi(2019). An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images. Engineering, Technology & Applied Science Research Vol. 9, No. 3, 2019, 4165-4168

[11] J. Joy and L. Koshy, "RubiCrypt: Image Scrambling Encryption System Based on Rubik's Cube Configuration," *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India, 2019, pp. 1-8, doi: 10.1109/ICSCAN.2019.8878785. keywords: {Encryption;Face;Image color analysis;Kernel;Real-time systems;Encryption;Rubik's Cube;Scrambling},

[12] M. J. Aqel, Z. AlQadi, A. A. Abdullah, "RGB Color Image Encryption Decryption Using Image Segmentation and Matrix Multiplication", International Journal of Engineering and Technology, Vol. 7, No. 3.13, pp. 104-107, 2018

[13] J. Thakur, N. Kumar, "DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol. 1, No. 2, pp. 6-12, 2011

[14] S. Wang, Y. Zheng, Z. Gao, "A New Image Scrambling Method through Folding Transform", IEEE International Conference on Computer Application and System Modeling, Taiyuan, China, October 22-24, 2010

[15] J. N. Abdel-Jalil, "Performance analysis of color image encryption\decryption techniques", International Journal of Advanced Computer Technology, Vol. 5, No. 4, pp. 13-17, 2016

[16] G. Ye, “An Efficient Image Encryption Scheme based on Logistic maps”, International Journal of Pure and Applied Mathematics, Vol. 55, No. 1, pp. 37-47, 2009

[17] Refregier P,JavidiB .Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 1995;20:767–9.

[18] P. R´efr´egier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20, 767–769 (1995).

[19] Z. Liu, Q. Li, J. Dai, X. Sun, S. Liu, and M. A Ahmad, “A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains,” Opt. Commun. 282, 1536–1540 (2009).

[20] Z. Liu, J. Dai, X. Sun, and S. Liu, “Triple image encryption scheme in fractional Fourier transform domains,” Opt. Commun. 282, 518–522 (2009).

[21] Z. Liu, M. A Ahmad, and S. Liu, “Image encryption scheme based on the commutation and anti-commutation rules,” Opt. Commun. 279, 285–290 (2007).

[22] R. Tao, J. Lang, and Y. Wang, “Optical image encryption based on the multiple parameter fractional Fourier transform,” Opt. Lett. 33, 581–583 (2008).

[23] X. Peng, H. Wei, and P. Zhang, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” Opt. Lett. 31, 3261–3263 (2006).

[24] Peng X, Zhang P, Wei H, Yu B. Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. 2006;31:1044–6.

[25] LiuW,YangG,XieH.Ahybridheuristicalgorithmtoimproveknown-plaintext attack on Fourier plane encryption. Opt. Express 2009;17:13928–38.

[26] RodriguezJAM,Rodriguez-VeraRR.Imageencryptionbasedonphaseencoding by means of a fringe pattern and computational algorithms. Rev. Mexicana De Fisica 2006;52:53–63.

[27] Liu Z, Dai J, Sun X, Liu S. Color image encryption by using the rotation of color vector in Hartley transform domains. Opt. Laser Eng. 2010;48:800–5.

[28] S. Li, Analyses and new designs of digital chaotic ciphers (Ph.D. Thesis), School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, Available online at ⟨http://www. hooklee.com/pub.html⟩, June 2003.

[29] Y. Matias, A. Shamir, A video scrambling technique based on space filling curve (extended abstract), in: Advances in Cryptology — Crypto'87, Lecture Notes in Computer Science, vol. 293, 1987, pp. 398–417.

[30] S. Li, C. Li, G. Chen, N.G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain text attacks, Signal Process.: Image Commun. 23 (3) (2008) 212–223.

PAPER NAME

2K22CSE03.pdf

WORD COUNT

8151 Words

CHARACTER COUNT

44397 Characters

PAGE COUNT

37 Pages

FILE SIZE

1.2MB

SUBMISSION DATE

May 29, 2024 9:08 PM GMT+5:30

REPORT DATE

May 29, 2024 9:08 PM GMT+5:30

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 4% Internet database
- 3% Publications database
- Crossref database
- Crossref Posted Content database

Excluded from Similarity Report

- Submitted Works database
- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 10 words)

2K22CSE03.pdf

My Files

My Files

Delhi Technological University

Document Details

Submission ID

trn:oid:::27535:60273896

Submission Date

May 29, 2024, 9:08 PM GMT+5:30

Download Date

May 29, 2024, 9:17 PM GMT+5:30

File Name

2K22CSE03.pdf

File Size

1.2 MB

37 Pages

8,151 Words

44,397 Characters

How much of this submission has been generated by AI?

0%

of qualifying text in this submission has been determined to be generated by AI.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?
The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.

Our testing has found that there is a higher incidence of false positives when the percentage is less than 20. In order to reduce the likelihood of misinterpretation, the AI indicator will display an asterisk for percentages less than 20 to call attention to the fact that the score is less reliable.

However, the final decision on whether any misconduct has occurred rests with the reviewer/instructor. They should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in greater detail according to their school's policies.

How does Turnitin's indicator address false positives?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be AI-generated will be highlighted blue on the submission text.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

What does 'qualifying text' mean?
Sometimes false positives (incorrectly flagging human-written text as AI-generated), can include lists without a lot of structural variation, text that literally repeats itself, or text that has been paraphrased without developing new ideas. If our indicator shows a higher amount of AI writing in such text, we advise you to take that into consideration when looking at the percentage indicated.

In a longer document with a mix of authentic writing and AI generated text, it can be difficult to exactly determine where the AI writing begins and original writing ends, but our model should give you a reliable guide to start conversations with the submitting student.