**Research Paper**

**IMAGE CRYPTOGRAPHY BY RUBIKS CUBE PRINCIPLE**

P.Sabiha – 17MIS0064 S.Swetha – 17MIS0084

**Guided By :**

Dr.Navaneethan.C

**Abstract :**

Cryptography is well known and widely used technique that manipulate information in order to cipher or hide their existence.

In the past years, a few encryption methods dependent on different algorithms have been proposed intended to secure digital pictures against cryptographic attacks. Chaos-based image encryption algorithms are generally used more often than others but require high computational cost. Moreover, this system is defined on real numbers whereas the cryptosystems are defined on finite sets of integers and also these systems are implemented using small key spaces which is insecure, especially in case of one-dimensional algorithms. The common image encryption algorithms such as DES, AES, RSA and the family of elliptic curve-based encryption (ECC) are also not helpful for fast and real-time communication applications for image encryption. Due to the high information redundancy some encryption schemes based on permutation have also been found insecure against various attacks.

In our project we are going to develop a code for more secure and fast encryption of

images using a unique image encryption algorithm based on Rubik's cube principle. The pixels of the image are shuffled in a way similar to that of a Rubik’s cube in a random manner using two randomly generated vectors. Then the same vectors are used for performing bitwise operation row-wise and column-wise. The XOR operator is applied to odd rows and columns of image using a key to decrease the association between original and encrypted images. The same key is flipped and applied to even rows and columns of image.

Finally, the algorithm which we used to develop the encryption system i.e.,Rubik's cube principle not only can achieve good encryption standards and perfect hiding ability but also can resist exhaustive attack, statistical attack and differential attack.

Various research, performance assessment tests and experimental tests done on similar type of image encryption algorithm shows it is suitable for real-time Internet encryption and transmission applications because of its fast encryption or decryption speeds it also demonstrates the robustness of the proposed algorithm against several types of attacks.

**Keywords:** Rubik’s cube algorithm, XOR operator, Chaos-based image encryption algorithms.

**Introduction :**

In the recent age, technology has moved leaps but it has also come with its downsides. One of them is illegal copying of digital intellectual property. Several works have been done to curb this issue. Some of the main ones are done by using encryption. This project focuses on using encryption for protecting digital images. Encryption is a process of transforming data into an unreadable format using certain algorithms to make sure that the data is available to only legitimate users i.e. only authorized parties can access the data.

The objective of this project is encryption of mainly digital images. There are already well known encryption methods such as symmetric-key algorithms (DES,AES,IDEA), asymmetric-key algorithms(RSA) and also algorithms based on Elliptic-curve-cryptography in place for data encryption but these are not the most suitable for image encryption. This is mostly applicable in real-time communication or in cases where fast encryption is needed.

The proposed encryption schemes in recent years can be mainly classified into categories as, value transformation, pixels position permutation, and chaotic systems.

Image encryption has been studied extensively. Some permutation-based encryption schemes have already been found to be insecure against certain attacks such as cipher-text only and chosen-plaintext attacks. It is due to the high data redundancy in such schemes and as secret permutations can be recovered by plaintext and ciphertext comparison,It is quite understandable. Although, chaos-based algorithms are used more often in image encryption in general, they have a high computational cost. Also, chaotic system are defined on real numbers whereas cryptosystems are defined on a finite set of integers.

In this project, we are going to consider the principle of rubik’s cube for image encryption. We are going to implement this algorithm which has been specified and extensively studied in the paper mentioned below.

**Related Work :**

Image encryption is a crucial issue in storing and exchanging different types of digital images. The main goal of any information security system is to protect confidential information against unauthorized access and attacks. Currently, we are generating a huge number of images. Governments and organizations have to deal with many sensitive and confidential images such as surveillance images, crime scene images, photos of suspects, military images, classified documents, medical images, etc. that should be stored, processed, and transmitted securely[1].Public elections are the basis of democratic societies. Selecting leaders and representatives by voting is the most important aim of this kind of government. Eligible voters must be sure that their votes are effective in their function. It is clear that in every election, one person or group wins and other candidates or groups are losers. Hence, after counting votes, there are often some complaints about voting regularity. Losers accuse the winning candidate or group to cheat on the votes[2].Steganography is a simple security method. Generally there are three different methods used for hiding information: steganography, cryptography, watermarking. In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical. Steganography is hiding information; this generally cannot be identified because the coded information doesn’t appear to be abnormal i.e. its presence is undetectable by sight. Detection of steganography is called Steganalysis. Steganography is of different types: 1. Text steganography 2. Image steganography 3. Audio steganography 4. Video steganography[3].Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). Steganography in these days refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person or persons view the object that the information is hidden inside, he or she will have no idea that there is any hidden information; therefore the person will not attempt to decrypt the information[4].

The advent of personal computers and the Internet has made it possible for anyone to distribute worldwide digital information. However, there are many applications that need to protect their information from people who can steal important data. Therefore, it is important to apply a method for hiding information, i.e., it is necessary to encrypt data. Traditional image encryption algorithms are 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)[5].Discrete Cosine Transform (DCT) constitutes a powerful tool in signal processing, since its first introduction (Ahmed et al., 1974). It belongs to a class of mathematical operations that includes the well-known Fast Fourier Transform (FFT), having as basic operation taking a signal and transforming it from one type of representation to another. More precisely, DCT transforms a signal from the spatial domain to the frequency space, with minimum information redundancy, since its kernel functions (cosines) comprise an orthogonal basis[7].The rapid growth of digital imaging applications, including desktop publishing, multimedia, teleconferencing, and high-definition television (HDTV) has increased the need for effective and standardized image compression techniques. Among the emerging standards are JPEG, for compression of still images [Wallace 1991]; MPEG, for compression of motion video [Puri 1992]; and CCITT H.261 (also known as Px64), for compression of video telephony and teleconferencing[8].Data compression has important application in the areas of data transmission and data storage. Many data processing applications require storage of large volumes of data, and the number of such applications is constantly increasing as the use of computers extends to new disciplines. At the same time, the proliferation of computer communication networks is resulting in massive transfer of data over communication links. Compressing data to be stored or transmitted reduces storage and/or communication costs[9].Data hiding techniques are considered very important roles with the rapid growth of intensive transfer of multimedia contents and secret communications. On the other hand, steganography is one of the most important information hiding techniques. By using steganography, information is hidden in carriers such as images, audio files, text files, and video files. In this paper, a modified steganography method based on the spatial domain is proposed[10].In recent years some scholars have overcome the barriers of harsh mathematics that chaos theory implies, more into practical and fun aspects of the reality (with its own tangled logic and math), proposing innovative digital image scrambling and ciphering schemes that are based on the rules sets of few of the most popular games. If it is to date the fruitful conjunction between games’ theory (namely, their rules’ design principles) and digital images’ cryptography (either classical or chaos-based) the going back would not make more than five years (i.e., a new-built and unique approach, which would crystallize in its early years, was identified)[11].During the past years the amazing developments in the field of network communications have created a great requirement for secure image transmission over the Internet. Since the Internet is a public network it is not so secure for the transmission of confidential images. Cryptographic techniques need to be applied to meet this challenge. Today security is an integral part of every technology and implementation. Cryptography is perhaps the most widespread form of secure communication. In this IT driven society. Image protection has become an important issue for communication of digital images through the networks. Encryption is the one of the ways to provide the security of digital images[12].During the past years the amazing developments in the field of network communications have created a great requirement for secure image transmission over the Internet. Since the Internet is a public network it is not so secure for the transmission of confidential images. Cryptographic techniques need to be applied to meet this challenge. Today security is an integral part of every technology and implementation. Cryptography is perhaps the most widespread form of secure communication. In this IT driven society. Image protection has become an important issue for communication of digital images through the networks. Encryption is the one of the ways to provide the security of digital images[13].Visual Cryptography is a technique that allows multimedia encryption so that the decryption becomes easy. It is a novel secret-sharing scheme that encrypts the image into ‘n’ shares that is the image is broken up into ‘n’ shares so that the receiver who has all the ‘n’ shares could only decrypt the image. While any receiver with ‘n-1’ share would not get any information about the original image. Because of increase in unauthorized usage of data and increase in hacking, the importance of visual cryptography has increased. It provides security to beat today’s authentication challenges and is very easy to implement[14].

**Proposed System :**

In the recent days image proceesing is the most used technique were the information should be hidden to everyone except to the authenticated access. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. There are so many Existing systems for the image cryptography like pixel transformation using rubic cube principle, a way for random image steganography, secure and verificable cryptographic scheme using rubic principle these are some of the existing systems of the image cryptography were in every system there are many advantages and also disadvanatges that is the reason to propose the new systems were the proposed system may not be perfect but it may decrease the disadvantages when compared to the existing systems.

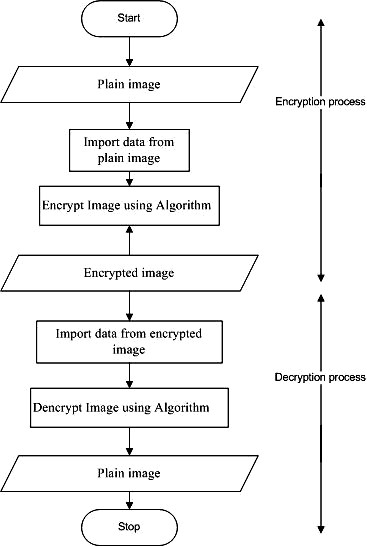
In the pixel transformation using the rubic cube principle is used to In this day and age of accelerated and convenient media for transmission and use of data resources the need for security has never been more profound and the methods that used in pixel transformation are implemented ethically or else the principle may not give the desired and the effective solutions which may lead to the wrong information.In a way for random image steganography, were it is a best method for hiding the data bulit creates complex in the security systems in encryption algorithm.

Where some image cryptography systems were implemented by using the AES, DES, ECC, DCT were they are most secure, Reasonable cost, Flexibility, Simplicity but these are common encryption techniques and also not helpful for fast and real-time communication applications for image encryption. Due to the high information redundancy some encryption schemes based on permutation have also been found insecure against various attacks.

So, the image cryptography using rubic cube principle the algorithm which we used to develop the encryption system i.e.,Rubik's cube principle not only can achieve good encryption standards and perfect hiding ability but also can resist exhaustive attack, statistical attack and differential attack.

**METHODOLOGY**

**Flow Chart:**



**Rubik’s cube algorithm:**

# **Encryption Algorithm**

Let 𝖨𝑜 = pixels values matrix of a 𝛼-bit grayscale image (𝑀×𝑁). Steps involved in encryption are:

1. Create two vectors 𝐾𝑅 and 𝐾𝐶 with random values of length 𝑀 and 𝑁, where the values in the vectors should be >0 and <2𝛼 -1. (𝐾𝑅 and 𝐾𝐶 should not have constant values )
2. Set the iteration value, ITERmax, and initialize the counter ITER at 0.
3. Increment the counter by one: ITER=ITER+1.
4. For each row 𝑖 of image 𝐼𝑜,
   1. compute the sum of all elements in the row 𝑖, this sum is denoted by

𝛼(𝑖)

(𝑖)=𝑁𝑗=1(𝑖,),𝑖=1,2,…,𝑀

* 1. compute modulo 2 of 𝛼(𝑖), denoted by 𝑀𝛼(𝑖),
  2. row 𝑖 is left, or right, circular-shifted by 𝐾𝑅(𝑖) positions (image pixels are moved 𝐾𝑅(𝑖) positions to the left or right direction, and the first pixel moves in last pixel.), according to the following: If 𝑀𝛼(𝑖)=0⟶right circular shift a. else⟶left circular shift

1. For each column 𝑗 of image 𝐼𝑜,
   1. compute the sum of all elements in the column 𝑗, this sum is denoted by

𝛽(𝑗),

(𝑗)=𝑀𝑖=1(𝑖,),𝑗=1,2,…,𝑁.

* 1. compute modulo 2 of 𝛽(𝑗), denoted by 𝑀𝛽(𝑗).
  2. column 𝑗 is down, or up, circular-shifted by 𝐾𝐶(𝑖) positions, according to the following:

Steps 4 and 5 above will create a scrambled image denoted by 𝐼SCR.

1. Using vector 𝐾𝐶, the bitwise XOR operator is applied to each row of scrambled image using the following expressions:

𝖨1(2𝑖−1,𝑗)=𝖨SCR(2𝑖−1,𝑗)⊕𝐾𝐶(𝑗),

𝖨1(2𝑖,𝑗)=𝖨SCR(2𝑖,𝑗)⊕rot180(𝐾𝐶(𝑗))

where ⊕ and rot180(𝐾𝐶) represent the bitwise XOR operator and the flipping of

vector 𝐾𝐶 from left to right, respectively.

1. Using vector 𝐾𝑅, the bitwise XOR operator is applied to each column of image 𝐼1 using the following formulas:

𝖨ENC(𝑖,2𝑗−1)=𝖨1 (𝑖,2𝑗−1)⊕𝐾𝑅 (𝑗)

𝖨ENC(𝑖,2𝑗)=𝖨1(𝑖,2𝑗)⊕rot180(𝐾𝑅(𝑗))

with rot180(𝐾𝑅) indicating the left to right flip of vector 𝐾𝑅.

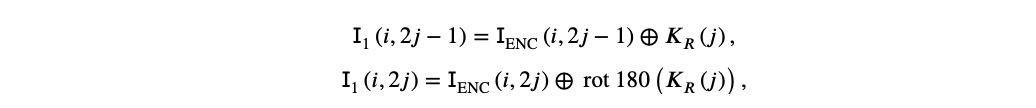
1. If ITER=ITERmax, then encrypted image 𝐼ENC is created and encryption process is done; otherwise, the algorithm branches to step 3.

𝐾𝑅, 𝐾𝐶 & ITER max are the secret keys.

# **Decryption Algorithm**

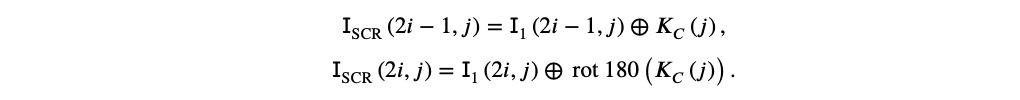
The decrypted image, 𝐼𝑜, is recovered from the encrypted image, 𝐼ENC, and the secret keys, 𝐾𝑅, 𝐾𝐶, and ITERmax as follows in the following.

1. Initialize ITER=0.
2. Increment the counter by one: ITER=ITER+1.
3. The bitwise XOR operation is applied on vector 𝐾𝑅 and each column of the encrypted image 𝐼ENC as follows:

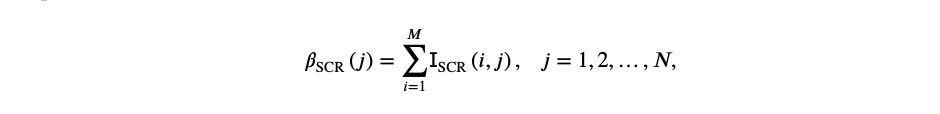


1. Then, using the 𝐾𝐶 vector, the bitwise XOR operator is applied to each row of image

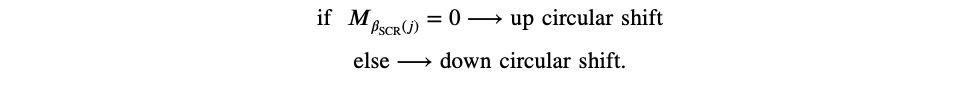
𝐼1:



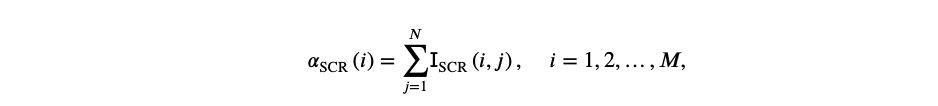
1. For each column 𝑗 of the scrambled image 𝐼SCR,
   1. compute the sum of all elements in that column 𝑗, denoted as 𝛽SCR(𝑗):



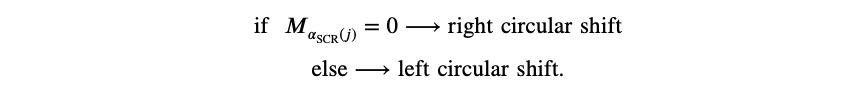
* 1. compute modulo 2 of 𝛽SCR(𝑗), denoted by 𝑀𝛽SCR(𝑗),
  2. column 𝑗 is down, or up, circular-shifted by 𝐾𝐶(𝑖) positions according to the following:



1. For each row 𝑖 of scrambled image 𝐼SCR,
   1. compute the sum of all elements in row 𝑖, this sum is denoted by 𝛼SCR(𝑖):



* 1. compute modulo 2 of 𝛼SCR(𝑗), denoted by 𝑀𝛼SCR(𝑗),
  2. row 𝑖 is then left, or right, circular-shifted by 𝐾𝑅(𝑖) according to the following:



1. If ITER=ITERmax, then image 𝐼ENC is decrypted and the decryption process is done; otherwise, the algorithm branches back to step 2.

**IMPLEMENTATION & RESULT**

**Sample Execution:**

**Input Image 1:**



('Vector Kr : ', [7, 114, 103, 17, 235, 153, 16, 86, 154, 178, 234, 144, 217, 215, 227, 32, 123, 71, 126, 165, 85, 70, 195, 250, 195, 161, 125, 137, 199, 1, 70, 15, 49, 207, 1, 33, 79, 180, 207, 229, 43, 193, 14, 105, 168, 14, 61, 203, 137, 23, 110, 226, 134, 0, 246, 240, 166, 71, 170, 225, 145, 76, 54, 187, 33, 95, 66, 137, 113, 204, 214, 164, 210, 142, 96, 167, 255, 207, 171, 120,

45, 25, 250, 232, 170, 13, 40, 94, 40, 213, 149, 182, 92, 35, 163, 121, 87, 72, 99, 229, 209, 236,

60, 204, 102, 103, 58, 227, 96, 94, 255, 26, 74, 196, 201, 196, 153, 20, 150, 153, 73, 68, 52, 229, 57, 223, 63, 180, 174, 15, 34, 77, 16, 28, 95, 167, 134, 173, 85, 21, 63, 111, 154, 170, 38, 10, 153, 40, 175, 165, 80, 92, 225, 174, 68, 85, 115, 246, 111, 10, 235, 201, 108, 61, 107, 82, 24, 134, 168, 215, 46, 106, 38, 182, 6, 85, 188, 142, 163, 182, 92, 124, 250, 148, 63, 38, 71, 70, 97, 223, 48, 96, 55, 5, 239, 246, 102, 192, 156, 54, 24, 69, 75, 75, 82, 250, 222, 25, 135, 162, 73, 20, 57, 176, 133, 67, 155, 80, 229, 203, 116, 29, 112, 20, 225, 200, 10, 178, 160, 54, 21, 247, 177, 56, 180, 58, 116, 19, 104, 139, 119, 86, 74, 24, 98, 201, 251, 6, 114, 145, 85, 118, 22, 93, 83, 116, 7, 222, 252, 193, 153, 160, 132, 5, 156, 165, 228, 114, 107, 129, 141, 255, 195, 102, 20, 59, 146, 128, 112, 207, 181, 210, 9, 57, 215, 57, 239, 39, 167, 102, 28, 39, 237, 113, 63, 15, 17, 146, 56])

('Vector Kc) : ', [136, 205, 248, 88, 246, 149, 160, 166, 50, 137, 246, 2, 252, 58, 6, 100, 176, 209, 82, 162, 190, 19, 48, 106, 225, 141, 93, 206, 148, 185, 148, 196, 102, 159, 128, 184, 247, 138, 204, 24, 110, 35, 88, 119, 221, 72, 27, 53, 213, 123, 48, 88, 246, 111, 188, 202, 191, 43,

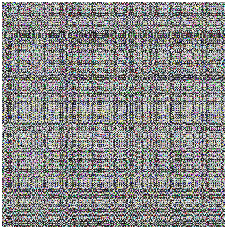
123, 210, 41, 176, 44, 24, 41, 88, 8, 32, 121, 192, 28, 176, 101, 102, 54, 222, 62, 92, 60, 2, 227,

135, 153, 150, 40, 200, 231, 198, 83, 234, 134, 160, 62, 151, 154, 250, 116, 123, 150, 3, 185, 60, 212, 232, 49, 68, 10, 16, 94, 65, 94, 31, 222, 142, 212, 173, 145, 250, 232, 162, 212, 36,

12, 72, 126, 246, 196, 48, 189, 192, 204, 90, 252, 254, 183, 137, 35, 203, 2, 252, 244, 241, 235, 226, 186, 113, 149, 6, 35, 47, 124, 13, 7, 207, 113, 60, 97, 198, 27, 192, 187, 187, 232, 242, 165, 108, 21, 31])

ITER\_MAX: 1

Encrypted image



Decrypted image:



**Conclusion:**

Finally we have done the encryption and decryption using Rubik’s cube algorithm, considering a image in the folder, which helps in security. Even this project can be developed in the future making the interface even better. This is all IMAGE CRYPTOGRAPHY BY RUBIKS CUBE project that we have done. So the Rubik’s cube algorithm is one of the efficient algorithms that are present right one in the field of Image Cryptography.

**References :**

1. Sirisha, M., & Lakshmi, S. V. V. S. (2014). Pixel transformation based on Rubik’s cube principle. Int J Appl Innov Eng Manage, 3(5), 273-277.
2. Amirtharajan, R., Abhiram, M. V., Revathi, G., Reddy, J. B., Thanikaiselvan, V., & Rayappan, J. B. B. (2013). Rubik's cube: A way for random image steganography. Res. J. Inform. Technol, 5, 329-340.
3. Nagarajan, B., & Manju, B.(2016) Secure And Verifiable Cryptographic Scheme Using Rubik’s Cube Principle. 4,198-205.
4. Abdullatif, A. A., Abdullatif, F. A., & Naji, S. A. (2019). An enhanced hybrid image encryption algorithm using Rubik’s cube and dynamic DNA encoding techniques. Periodicals of Engineering and Natural Sciences, 7(4), 1607-1617.
5. Moayed, M. J. (2009). Voter Verification Using Rubik's Cube (Doctoral dissertation, Universiti Putra Malaysia).Universiti Putra Malaysia,1-25.
6. Venkata krishna.K.P., Hemanth.v.,& Vishnu.R.,Agilandeswari.L.,Novel secure technique using visual cryptography and advance AES for images. International Journal of Knowledge Management & e-Learning,2016.1-7.
7. Savitha.B., (2017). ‘Image Steganography’.Wright State University,1-17.
8. Dr Ekta Walia, Payal Jain and Navdeep. “An analysis of LSB & DCT based Steganography.” Global Journal of Computer Science andTechnology, April2010.v-10.4-8.

[9]Elena.A.,Antonia.A.,Fabiola.M.,Angel.M., Associative Models for Encrypting Monochromatic Images.1-2.

[10] G.A. Papakostas, D.E. Koulouriotis and E.G. Karakasis (2009). Efficient 2-D DCT

Computation from an Image Representation Point of View, Image Processing, Yung-

Sheng Chen (Ed.), ISBN: 978-953-307-026-1, InTech,

[11] Parkhi, Disha And Lokhande, S. S. (2012) "Image Compression System Using ANN," International Journal Of Computer And Communication Technology: Vol. 3 : Iss. Article 4. <https://Www.Interscience.In/Ijcct/Vol3/Iss1/4>

[12] Shanmuganathan, Sankar. (2017). Cte: A Method To Compression-Then-Encryption For Images. International Journal Of Engineering Sciences & Research Technology. 6. 214 .

[13]Rekha,Goudar,Rohit(2018).Secure Secrete Image Carrier Using Rubiks Cube.Volume 120 No. 6 2018, 12111-12122 ISSN: 1314-3395 .

[14] Vyom Chhabra, Tejeswini Sundaram. Binary Encryption Based On A Rubik's Cube.

[15] Seetaiah Kilaru, Yojana Kanukuntla, Asma Firdouse, Mohammad Bushra & Sindhu Chava(2013). Effective And Key Sensitive Security Algorithm For An Image Processing Using Robust Rubik Encryption & Decryption Process.

[16] Adrian-Viorel (2015). .Kenken Puzzle – Based Image Encryption Algorithm.

[17] Lini Abraham1 , Neenu Daniel2(2013). An Improved Color Image Encryption Algorithm With Pixel Permutation And Bit Substitution.

[18] H. Sharma, N. Kumar And G. K. Jha, "Enhancement Of Security In Visual Cryptography System Using Cover Image Share Embedded Security Algorithm (CISEA)," *2011 2nd International Conference On Computer And Communication Technology (ICCCT-2011)*, Allahabad, 2011, Pp. 462-467, Doi: 10.1109/ICCCT.2011.6075137.

[19] K.A.Abitha Pradeep,K.Bharathi(2016) Secure Communication Based On Rubik’s Cube Algorithm And Chaotic Baker Map. [Volume 24](https://www.sciencedirect.com/science/journal/22120173/24/supp/C), 2016, Pages 782-789.

[20] Krutika Solanki , Vidisha Vankani, Pooja Pukle, Sridhar Iyer(2016). Multimedia Encryption Using Visual Cryptography.