IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Secured Image Encryption Algorithm BasedOn Rubik's Cube Principle with RSA Encryption

Karpagalakshmi M
Information Technology
National Engineering College Kovilpatti, India

Saravanan B

Information Technology
National Engineering College Kovilpatti, India

Dr.L. Jerart Julus
Information Technology
National Engineering College Kovilpatti, India

***Abstract*—Due to the sensitive nature of photographs, it is sometimes essential to encrypt their transmission. In recent years different encoding methodologies were mostly based on the chaotic, which helps to secure digital images against many cryptographic assaults. Because these types of encryption techniques often have a limited amount of key area and so provide less security, especially if they are not consigned if it is 1-dimensional. We introduced a unique picture encoding methods based on the Rubik's cube with RSA algorithm in this work. The Rubik's cube concept is used to clutter the earliest image. With the help of two secret keys the RSA technique applies the XOR operations. The earliest image is cluttered and XOR operations are used to encrypt it, and then it gets decrypted in a similar way. This technology offers a more secure procedure for assuring the security of picture data, which may even be saved on the cloud. It has been tested on many types of photos, and the final output has been reported. At last, the experimental findings show the well-built encryption and have protection ability, but it also withstands intensive, statistical as well as differential assaults.**

Keywords- RSA encryption, Rubik's Cube, Image Encryption

I. Introduction

As papers and equipment became more widely utilized in numerous sectors, the end of the twentieth century saw an unprecedented technological shift from analogue to numerical. However, the advantages of this computerized world did not come without a price, such as unauthorized cloning and distribution of data. To handle this thing, academics were more driven to develop innovative and effective document protection strategies for multimedia documents.

Various encryption and information concealment techniques have been implemented in this situation. The first entails altering multimedia materials using an algorithm to render them unintelligible to all but legitimate users. The second way is to embed digital information in multimedia publications to verify that the digital multimedia information's are owned and maintained.

Now a days, there is an enormous development in securing the data over the network field. It is not suitable to share the privileged picture or data over the internet. Various cryptographic techniques have been introduced to handle this kind of problem over internet. It is important to protect the data share via internet. For attaining secure transmission, we must hold an cryptography as a tool. For ensuring the security we go for encryption.

The original image is encoded using encryption, that encoded image is difficult to understand. No one should be able to view the content inside. With the help of decryption key, we can view. Only a known user can render it with the help of key. Secure transmission exit in cable television, military image communications, and so on.

A. Cryptography

Cryptography is a means of protecting data from unknown access. By using algorithm, we can convert the plaintext which is raw data into cipher text with the help of encryption key. With the help of decryption key, we can convert the ciphertext into human readable format. Image protection is of special relevance in this piece. For faster and live communication, traditional image encoding algorithms may not be the ideal choice for image encoding.

B. Feature of Cryptography

Below is a list of them

1) *Confidentiality:* No one can access the dataonly authorized person can access it.
2) *Integrity*: Simply refers to the trustworthiness of data while sharing via internet.
3) *Non-repudiation:* Someone cannot deny the validity of something.
4) *Authentication:* Simply refers to the confirmation of source and unification of data.

C. Types of Cryptography

1) *Symmetric Key Cryptography:* With the help of single shared key, Alice and Bob will encrypt the data. We should exchange the keys int a secure manner.

2) *Hash Function:* Based on the plain text, a hash value will be defined in a particular length and that will bedifficult to reconstruct the plain text's i.e., raw data.

3) *Asymmetric Key Cryptography:* With the help of pair of keys (i.e., public and private key) we can encrypt and decrypt the data.

D. Components of Cryptography

A simple cryptosystem consists of the following elements:

1) *Plaintext:* This is the original data that has to be kept safe while being transmitted.

2) *Cipher text:* It is a text which human cannot understand. It doesn’t make any sense, which is created by an encryption algorithm.

3) *Encryption Algorithm:* From the raw data, we can produce a cipher text with the help of encoding key.

4) *Decryption Algorithm:* With the help of decryption key, we can produce a data which is understand by a human.

5) *Encryption Key:* Key that possess a piece of information, used to encode the raw information.

6) *Decryption Key:* Key that possess a piece of information, used to decode data from cipher text.

A key space is a collection of all potential decryption keys for a given cryptosystem.

E. Cryptographic Attacks

The primary purpose of a hackers is to break a cryptosystem and retrieve the data. In case a key is identified by the hackers means, that system will be controlled by the hackers.

It is classified as follows based on the methods used:

- Ciphertext Only Attack (COA)
- Known Plaintext Attack (KPA)
- Chosen Plaintext Attack (CPA)
- Dictionary Attack
- Brute Force Attack (BFA)
- Man in the Middle Attack (MIM)
- Side Channel Attack (SCA)
- Timing Attacks
- Power Analysis Attacks
- Fault Analysis Attacks

II. Related Work

Based on repetition of random phase encoding, Liu et al. [1] suggested an encoding for picture which approaches gyrator transformation. Images are in iterative structure which helps to encrypt more phases. Computer and a 2-dimensional chaotic mapping were mostly used by random phases. For storing a data and transmitting a data in real time implementation mapping relation is much better compared to traditional approach.

Guo et al. [2]. Color image is converted into IHS model. DFRNT is used to encode the depth of the component, which is a type of encryption that protects both the value and thespotof picture element at the same time. It saves storage capacity compared to double-random-phase pattern. Same level of security is maintained for both the encoding and decoding phase.

An image encoding technique has been introduced by Z. Liu et al. [3],Which is mostly based on the gyrator and Arnold transform. Single Image is divided into various small substitute images. After that image are cluttered. With these methods we just enhance the security level. We can clarify the security and validity with the help of simulation technique. Tao et al. [4] put forth an image encoding techniquethat can be used for different picture encoding which is based on (FRFT-Fractional Fourier Transform). Compare to FRFT this type of encoding usewider key area. Transformation orders is very sensitive while decryption of image occurs.

Fractal circuit structure for spatial decorrelation of image is introduced by Zunino [5]. With the help of Hilbert curves to build a circuit in efficient manner in designing phase which eliminates the correlation. This technique is mostly used in various areas of data processing. Zhang and Liu [6] proposed an image encoding method based on rearrangement. This approach rearranges the pixel of that image. Skew produces the keystream that will connected to the plain image. It can be observed that this methodology is economical and dependable, having a robust potential to be used in internet security and safer transmissison.

In image encoding, Zhao and Chen [7] suggested using an Ergodic matrix. This study examines ergodic matrices and their applications in digital picture scrambling and encoding. With the help of permutation algorithms, they execute it. In addition to that, they investigate the isomorphism link between ergodic matrices and permutation groups. Finally, they are used to encrypt the photographs. The preliminary results are encouraging.

Zhu et al. [8] made a view on encryption with bit-level permutation based on confusion-diffusion architecture. When a bit in pixel is transferred to another pixel, the values get modified. The Performance has been compared with pixel-level-cipher and bit-level cipher. The results signify the increased efficiency of the cryptosystem.

Huang and Nien [9] presented a pixel shuffle based on Multi chaotic systems for image encoding. To assess the security analysis, statistic approaches and the correlation coefficient are used. At last,speculativeimage are used as examples to demonstrate that the suggested approach has superior encoding performance and reach the high confidential security.

G. Chen et al. [10] map-based image encoding technique based on 3D. This scheme uses 3D cat map to shuffle the position and to differentiate cipher-mage and plain-image. It is suitable for transmission applications and real time-internet image encoding applications. The results clearly employ the rapid speed and security on encoding.

III. Existing System

In the persuasion of the DES algorithm, the unstable series formed by Chua's circuit is used as the leading pivotal [4].By applying the XOR performance between unstable series of alternate-key and cleartext, the novel computation may successfully adjust the firmness of unencrypted text which move in 16-round format. As a consequence, the key space is intensified, and the aggressive to attack sense is modified for epic force offence and tangible offence. To begin, the encoded entity is chosen as a picture/The following is a detailed description of the encryption process.

1) *Data Block:* The image data should be divided into 64-bit cleartext pieces. Initial transformation divides a chunk of 64 bits decisions data into a 32-bit left alternate-chunk (L 0) and a 32-bit right alternate-chunk (L 1)

2) *Key Generation:* By creating Chua's area's beginning value and producing unstable series, you may produce 64-bit info as the original chunk and another 48-bit info as Chua's. The original chunk is modified to 56-bit info, then divided into 28 bits on the nigh side (C) and 28 bit on the right-side of (D), C and D are placed into 16-disk left convention, and the outcomes after each convention is transposed under choice-two modified yielding the 48 bit alternate-key K I.

3) *16-disk construction:* The sources of the 16-disk iteration in the 16-disk formatter are L I and R I. When a 32-bit R I is substituted with an F-function, the data is first enlarged to 48 bits, then the 48-bit R I KI and data are XOR in sync, and the F-function outcomes is formed following s-box and P modification. Finally, the next sources will be determined using the iterative technique below.

4) *Left and Right Interchange:* Swap L15 and R15 after the 16-disk phase is finished.

5) *Outcomes Findings:* An inverse beginning modification is used to convert the left and right interchange outcomes, yielding a encoded image. It uses less key space than DES. The first key is resistant against brute force assaults since it is generated via the Chua route. Picture Encoded algorithm, the system is based on a unique unstable mixed system:

This paper presents a new mixed tumultuous system. The approach is a nonlinear combination of common chaotic maps like the Logistic and Sine maps. The Chaotic systems' interactions are regulated by the encoded keys.

IV. Proposed Systems

The notion of Rubik's cube is used to suggest a revolutionary picture encryption technique. The original picture is jumbled using the Rubik's cube method. The RSA technique then applies the XOR operator to the scrambled image's rows and columns using two secret keys. Asymmetric encode techniques is achieved by using RSA techniques. It possesses two independent keys. The General Key is made available to everyone, but the Secret Key, as the name suggests, is kept hidden.

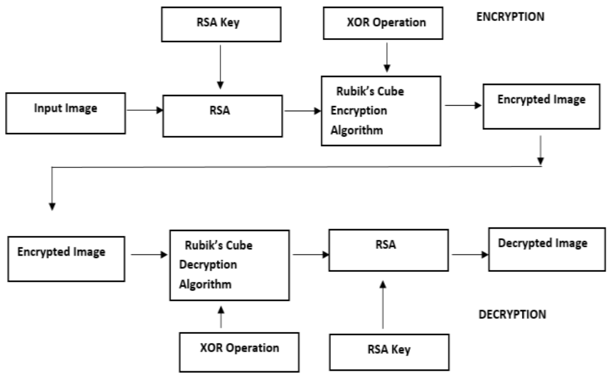


Fig.1. Block Diagram

In the proposed RSA system the user needs to specify the two prime integers for key generation which are described as p and q. For, generating the key the product of two prime integers p and q which is stored as n(i.e) n=p*q . The p and q must be chosen around length of 155 to ensure the highest level of security as it reduce the finding of predicting the p and q by someone. Hard numbers make easier to protect the data at the same time it ensures higher security.

After choosing two prime numbers p and q , the user needs to select an arbitrary number which needs to smaller than product of relative primes p and q. after choosing an random integer we can get an product 'e'.Where e is the product of p and q with common factor 'l' . when it is divided by least common multiple a new integer 'd' is derived which can be obtained only when the remainder of p and q divided by common multiple leaves '1' as residual. The number 'd' can be also determined using Euclidian theory if p and q is well known. It is impossible to determine whether 'e' or 'd' is given with out 'p' and 'q'. Both 'p' and 'q' are important as it is core factor to determine the RSA key.

The two integers 'd' and e' are mainly used to exchange keys between users. Moreover the keys are shared publicly. When a user X try to exchange confidential information to another user Y both share their 'd' values privately .When X send his message with publicly with 'n' and 'e' , the Y decrypts it using 'd' which was shared previously. In this way the transmission of message is done securely. As it improves the Secure Data Transmission among the users.

Data Transfer between two user can be done by verifying the secure communication. User X makes an authenticating channel by making 'n' and 'd' publicly while making 'e' as secure. User B confirms that channel is secure by sending an encrypted message to A which can be decrypted only by A using 'e'.On decrypting if B receives successful decryption by 'A' , 'B' can confirm that 'A' is the right person to share the message confidentially, because 'A' has 'e' which is used as an decrypting key by both users. Moreover the message can be digitally signed using Hashing Function. This method involves conversion of messages into digest bits and mixing with other bits which results as half interchanged in crypto-safe manner.

A identifies a statement that may or may not need to be respected and protected by encrypting the digest with the hidden e and attaching it to the payload. Anyone may then read the content and obtain the hash using the shared key d, which he can estimate autonomously from the text. If they agree, he must consider that A devised the cypher since only A could decode the info because only A understood e.

In all proposed two-key cryptosystems, the splitting of the seclusion or opacity route from the validation or verification route has come at a substantial expense up until now. The asymmetric encoded/decoded process necessitates significantly more effort, resulting in a significant reduction in available bandwidth (Data is transferred in bits per sec). Single-key algorithms have been able to achieve a sources 1,000 to 10,000 instances. For the past twenty years, two-key algorithms for equivalent safe systems have outperformed .As a result, the most popular use of two-key cryptography is hybrid systems.

In such a system, a two-key approach is used for access control and message authentication, or to interchange a procedurally chosen session key for use with a single method for primary assertion at high speed. At the conclusion of the session, this key is discarded.

A. *Security Analysis*

Security is a major concern in cryptography. A good picture encryption method should be able to survive attacks such known normal text, encoded-text-only, statistical analysis, and brute-force. In this part, the recommended photo encoded approach is put through its paces. Security was assessed using quantitative models and sensitive data research.

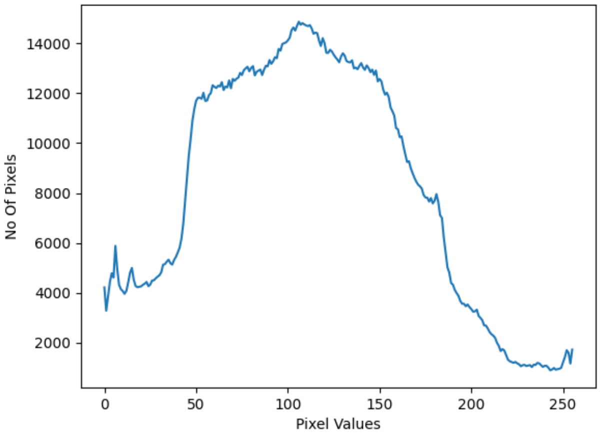
B. *Key Space Analysis*

A reliable pictorial encoding approach must have a large key space in order to render brute-force assaults effectively (quantitatively) unfeasible. In theory, the proposed approach can manage an endless key space. In our technique, however, the encoded key is formed up of the (KR, KC,ITERmax) triplet. For a -tiny Io is a source image with a dimension of MxN units, the dimensions KR and KC have 2M and 2N possible values, respectively. When both dimensions must have semi values and the key space size is 2(M+N) xITERmax-22 keys, it is evident that the key area may be enlarged when the number of repetition of ITERmax is enlarged. For instance, using ITERmax=1 and a 256x256 pixel 8-bit scale grey image. The sensitive data size is 24096-216≈101233, which is larger than the proposed image encoded algorithms' key regions and wide enough to survive rigorous attack.

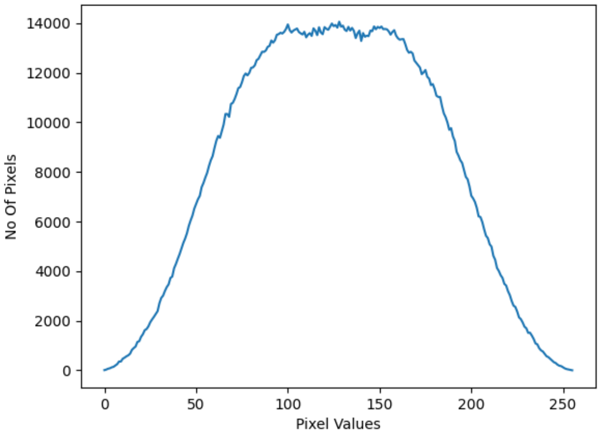
C. *Key Sensibility*

Encoded techniques would be sensitive to the encoded key: any small modification in the key should cause a significant modification in the encoded(or decoded) image. Two studies were carried out to highlight the method's primary sensitivity. The first shows how a change in the key impacts the encryption of a photograph. Here, the primary image, is encoded with the value K1=(KR,KC,ITERmax), where KR, KC, and ITERMAX are all produced in a driftless way. The same image, is then encoded using a new value, K2, which differs from the previous value, K1, only in the least significant bit, i.e. K2=(KR,KC,ITERmax+1). This observations is repeated 100 times, each time with different value pairings K1 and K2 (still it differs by the less representative bit). The values for the encoded photo with key K1 and the encoded picture with key K2 using 100 distinct key pairs are shown in the table, along with their mean and standard deviation. The mean NPCR values are near to 100 percent, showing that the image encoded with key K1 differs representative from the image encoded with key K2. In addition, the standard deviation values are low, denoting that the NPCR values are closely bounded by the mean value.

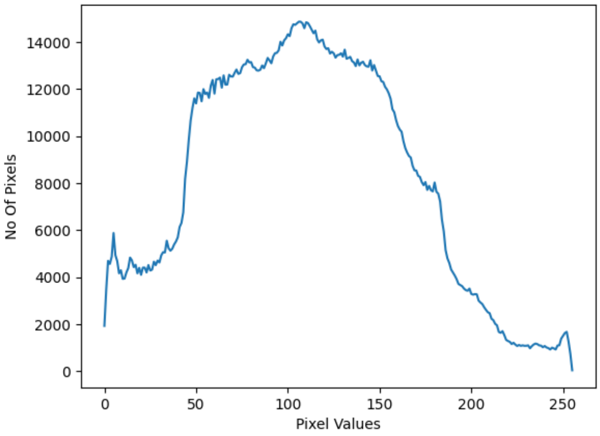
V. Result



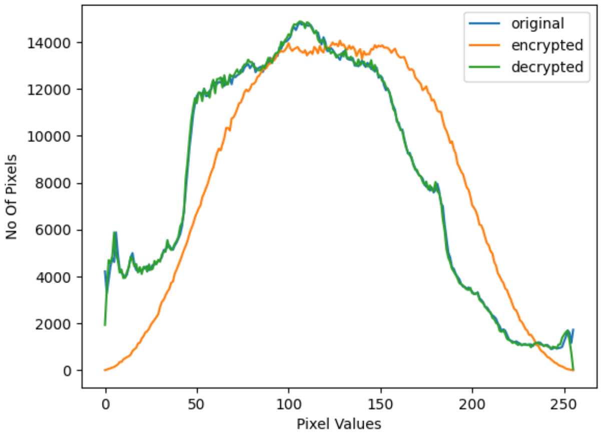
Original Image



Encrypted Image



Decrypted Image



Combined Result of Encryption, Decryption and Original Image

VI. Conclusion

The RSA algorithm and the Rubik's cube idea were used to create an encryption mechanism. The security level may be increased with the help of this approach. It's straightforward and produces decent permutation and diffusion processes in a fair amount of time. The suggested approach will give various benefits over current solutions in terms of picture encryption. The technique gives the user freedom by allowing them to encrypt a broad variety of pictures. The programmed allows you to choose from a variety of standard format photographs in any shape or size. This algorithm provides lossless encoding as well as decoding. During these processes, none of the data get lost. The image quality is also preserved. This method commute picture pixels using the Rubik's cube concept. With the help of XOR operation we can perform odd rows and columns of a image to execute a connection between earliest image and then the encoding image. The process is reversed for an image and the similar key is used to apply for even number of rows and columns. The analysis was used to conduct various experimental results to decrease the attacking vectors of image encryption by making the data hiding techniques more secure for the future. Furthermore, experiments show that the proposed picture encryption technique is quite safe. It also has quick encoding/decoding capabilities, making it ideal for live encryption and sharing of image over internet.

Acknowledgment

First and probably most important, we'd like to convey our profound gratitude to everyone who assisted us in completing this project. We overcame several obstacles during the completing process. However, others aided us in overcoming these challenges. We are grateful to Dr.L. Jerart Julus sir for his kindness and supervision. Our team was able to learn all elements of project work as a result of his involvement.

REFERENCES

[1] Z.Liu,L.Xu,C.Lin,J.Dai,andS.Liu,“Imageencryptionschemebyusingiterativerandomphaseencodingingyratortransformdomains,”OpticsandLasersinEngineering,vol.49, no.4,pp.542–546,2019.

[2] Q. Guo, Z. Liu, and S. Liu, “Color image encryption by using Arnold anddiscrete fractional random transforms in IHSspace,” Optics and Lasers inEngineering,vol.48,no.12,pp.1174–1181,2020.

[3] Z.Liu,H.Chen,T.Liuetal.,“Imageencryptionbyusing gyratortransformand Arnold transform,” Journal of Electronic Imaging, vol. 2, no. 4, pp.345–351,2011.

[4] R. Tao, X.Y. Meng, Andy. Wang, “Image encryption with mul-tiordersof fractionalFouriertransforms,”IEEETransactionson InformationForensicsand Security,vol.5,no.4,pp.734–738,2018.

[5] R.Zunino,“Fractalcircuitlayoutforspatialdecorrelationof images,”ElectronicsLetters,vol.34,no.20,pp.1929–1930,2019.

[6] G. Zhang and Q. Liu, “A novel image encryption method based on totalshuffling scheme,” Optics Communications, vol.284, no. 12, pp. 2775–2780,2020.

[7] X.Y.ZhaoandG.Chen,“Ergodicmatrixinimageencryption,”inProceedings of the 2nd International Conference on Image and Graphics,vol.4875,pp.394–401,August2019.

[8] Z.-L.Zhu,W.Zhang,K.W.Wong,andH.Yu,“Achaos-basedsymmetricimageencryptionschemeusingabit-levelpermutation,”InformationSciences,vol.181,no.6,pp.1171–1186,2019.

[9] C.K.HuangandH.H.Nien,“Multichaoticsystemsbasedpixelshuffleforimageencryption,”OpticsCommunications, vol.282,no.11,pp.2123–2127,2019.

[10] G.Chen,Y.Mao,andC.K.Chui,“Asymmetricimage encryptionschemebasedon3Dchaoticcatmaps,”Chaos,SolitonsandFractals,vol.21,no.3,pp.749–761,2020.