

# Securing Images through Cipher Design for Cryptographic Applications

Punya Prabha V<sup>1</sup>

Electronics and Communication  
Engineering, Ramaiah Institute of  
Technology Bangalore, INDIA

Dr. M D Nandeesh<sup>2</sup>

Electronics and Instrumentation  
Engineering, Ramaiah Institute of  
Technology, Bangalore, INDIA

Tejaswini S<sup>3</sup>

Medical Electronics and Engineering  
Ramaiah Institute of Technology  
Bangalore, INDIA

**Abstract**—The emphasis of this work is image encoding based on permutation as well as changes that utilize Latin cube as well as Latin square image cipher meant for both color and gray images. Generally, multimedia data are transmitted in the network as well websites, numerous methods have been established for securing the information without any negotiation. Security of information in all the areas is required to ensure that the information sustains privacy, is presentable for recovery as well as governance purposes. These data can be secured by taking CIA (confidentiality, Integrity, and Availability) to realize information like confidentiality about the data that can be reserved as undisclosed from an illegal user of source, the integrity of the data is maintained unaffected for unauthorized font, availability of resources for official personal to retrieve data for access the information. Authentication of a person is by identification, conserving information and its validation of data. Implementing this authentication will store the data in the required format that is either exchanged or transmitted for the internet application. By breaching the misuse of data is can be protected for confidential as well as sensitive data. To achieve security and maintain confidentiality cryptographic methods are implemented.

**Keywords**—Decryption; encryption; Latin square generator; sequence generator

## I. INTRODUCTION

In the current scenario security of data is the main issue to maintain confidentiality as well as privacy. The main concern is managing the data while communicating as well as storing data from stealing as well as exploiting the data. For this purpose, an appropriate method has been employed for securing the data while transmitting as well as storing the data by utilizing the technique of cryptography. The information is utilized in the form of a plaintext image. The encryption technique converts this plaintext image into an unidentifiable form that cannot be easily decoded. By employing the decryption process, it is possible to get back original information by utilizing the Cipher text method. The main solicitations of this image encryption are many, some of them are military application, medical images, communication via the internet and many more. In this electronic era, cryptography is applied to provide various types of security to different electronic devices [1]. New encryption for images that utilize permutation-substitution network and chaotic systems has provided a better result in terms of both

qualitative and quantitative studies that is superior to other techniques [2]. Generally, an intelligent technology that can protect the information from unauthorized person to hack or decode, that the data is immune to attack. This will implicate various techniques such as decipherment in symmetric and asymmetric keys [3] [20]. This process uses the decryption and encryption of data that is equivalent to electronic locking of knowledge [4]. This technique uses a private or secret key that can be shared only with receive for decoding as well as encoding the information. A novel technique based on memristive chaotic for random behavior is used for encryption has resulted in effective results in the decryption and protecting the data [5] [16]. The behavior of chaotic systems is mainly categorized using sensitivity based on dependence on primary situations. By using this chaos for self-synchronization has ignited a huge work in the field of cryptography [6] [15]. For certain initial conditions, some nonlinear functions can generate chaotic or random numbers. By utilizing a one-time pad system and replacing it with proper chaotic function cryptographic results can be improved [7]. Encryption of probabilistic image for LSB plane using random noise provides better diffusion as well as confusion properties with error tolerance [8] [10]. The security analysis is tested for different types of attacks [9] [18]. Decipherment of plain text is called secret information of plain text  $p$  and cipher text  $C$  is encrypted [11]. Latin square and CNN, for the input image are implemented bitwise and encrypted and decomposed to obtain encrypted image [12] [17]. Input image based on Latin Square creates 256 bits' key, which is operated by ex-or with Latin square to obtain encrypted images [13]. Latin rectangle scrambling using chaotic map reduces the number of iteration for achieving better security [14]. Latin square with S box and chaotic system results in better security [19]. For decryption, decoding the cipher image accompanying lookup table with index numbers results in effective and secured results [21]. Images of multimedia and its application are focused on efficient encryption and decryption to obtain better results [22].

This article is organized as follows, Section 2 provides the background of encryption methods. Section 3 explains the methodology of implementation of Latin square that generates and Substitution for cipher image as well as Whitening of premature images. Whereas Section 4 provides and evaluates the results and Section 5 concludes this paper.

## II. BACKGROUND

With the evolution of information technologies and pandemic situations, present days, people have started to use the internet and images in their daily routine. So encryption of images is gaining huge momentum for the present situation. For security reasons, image encryption converts the original images into unrecognizable images, Medical images, military services as well as its affair application, e-commerce, telecommunication, and many applications that gains the prominence of image encryption. In the present scenario, usage of text data has been reduced because of the advantages of the security in the digital images, since a different enormous amount of information like wide content, maximum data, as well as monotony and an exceptionally authoritative correlativity, can be obtained by the neighborhood pixel.

### A. The Objective of the Work

Cryptography deals with mainly three core capacities like integrity, authenticity and confidentiality, which defends the digital data from hackers or unauthorized users from theft. By using encoding, the confidentiality of information is hidden is known as data privacy. The private key is used to extract the image at the transmission of the data. For the decryption of information, the same private key is used that has been used for encryption. Authenticity assurances that a person or a process can be identified receiver by their identification method. If the same data has been transmitted to the receiver ensure that data is integrated, without loss of any information sent by the transmitter.

## III. METHODOLOGY

Misuse and theft of information are the main threat while storing and transmitting images, to a major amount of care has to be taken to maintain confidentiality and privacy. A technique based on cryptography can be utilized to store information as well as communication of data in plain text data. The process regarding hiding a given message as a fragment of a specific kind with accurateness to protect the data is encoding. The technique of converting cipher content back into plain text without any loss is deciphering.

As a part of security and confidentiality, the encrypting technique has gained momentum in the present situation. Information safety is a significant subject as part of communication purposes and for image storage, encryption is a distinct behavior that can secure the information. For this purpose, encrypting has enormous applications Image encoding includes a huge number of applications Encrypting text messages may lead to unrecognizable information or trash data known as cipher content. This technique is utilized to guarantee that data hidden from others of concern is not intended to, furthermore, individuals can recognize the encoded data. The technique of recovering the cipher text to its reliable plaintext is known as decryption.

### A. Latin Square

A Latin Square is a collection  $N \times N$  is jumble-sale of demonstration of  $N$  different elements, that all the elements

representation considering exactly just the once in each distinct row along with each distinct column. Fig. 1 represents an example of a Latin square.

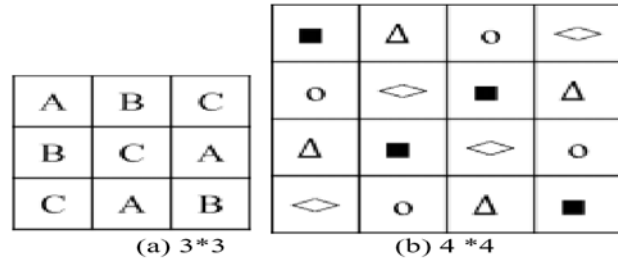


Fig. 1. Latin Square with Dissimilar Sets and Orders.

### B. Latin Square Generator

A Latin square is created by using two structures of identical length. If  $P1$  and  $P2$  are two sequences of length equal to  $N$  arrangements [11].

$LS = LSG(P1, P2)$

$P1$  and  $P2$  are input sequence

Ensure: -  $LS$  is a  $N$  order Latin square

$S1 = \text{Sort Map function}(P1)$

$S2 = \text{Sort Map function}(P2)$

For  $i=0$  to  $N-1$

$LS(i,:) = \text{Row shift}(S1, S2(i))$

End

$P1$  and  $P2$  are two input sequences that are aimed to generate a pseudo-random number generator. Sort Map function ( $S1, S2$ ) is classifying function with index in the middle of an  $S1$  and  $S2$  series, as a sequence of acclivitous order can be obtained by transformed edition  $S1^*$ , and operated on Row Shift is through ( $S1, v$ ) which is a periodic transfer of the  $S1$  arrangement with  $v$  elements to the left [9][10][11].

### C. Substitution-Permutation Network

Input information in cryptography is represented as plaintext and the resultant output information is called cipher text. A substitution-permutation network (SPN) is a sequence of cipher that includes various iterations, for each iteration includes a replacement, a variation and an additional key. It is a sequence of mathematical equations utilized for block cipher or different algorithms. Block ciphers algorithms are designed employing replacing and variation in various forms of SPN. Throughout the  $N$ -iteration variation and replacement of the given network, a plaintext will be converted into a new bit series and symbolized as  $P$ , which is primary and source content that has to be encoded. SNP that has been encoded to obtain the cipher text in the bit sequence  $C$ , by using this technique. Fig. 2 represents the substitution permutation network. A commonly used procedure to persistently synthesis with a given key for the plaintext is known as Latin square

whitening. Replacement of one byte to other bytes in the input sequence is known as Latin Square Substitution. Whereas shuffling bit location in the input sequence is done in Latin Square Permutation. Similarly, the reverse will be implemented in the decryption process of a substitution and permutation network cipher.

#### D. Latin Square Image Cipher

In the encoding and decoding technique for cipher, the treatment block is by splitting (32\*32) bytes of segmented grayscale, for which its definite pixel value with the intensity of 256 levels (1byte). In this algorithm P is a plaintext image is to be defined by (32\*32) byte, whereas cipher image C is denoted by (32\*32) byte, Latin Square is denoted by L (32 bytes), and the encoding key is denoted by K (32 bytes) encoding key. This suggested technique iterates for 4 and 8 rounds of substitution as well as permutation network structure respectively. Fig. 3 represents Latin square image Cipher with 8-round SPN.

#### E. Latin Square Whitening

By utilizing a typical SPN method for ciphers block, the mixing of the content of plain text P along with key using

rotation is implemented by using logical operations such as XOR procedures. In this proposed algorithm plain text P is composed of 1byte per pixel for the encoding process. In a normal predictable technique, logical whitening using XOR turns out to be intolerable, because of unsuccessful of information in images. Mixing the content of plaintext with that of a sequence is the to generate the Latin square is intended in whitening, for this purpose cipher is reorganized through Finite field or Galois field for plain text image that can be represented as

$$f = [r + 1] 2^8$$

The reverse of whitening technique to obtain Latin square can be obtained by using this equation,

$$r = [f + 1]2^8$$

Where f is the whitening result in the byte.

l is the Latin square in the byte.

r is a plain text image in the byte.

$2^8$  is used to calculate Galois or finite field.

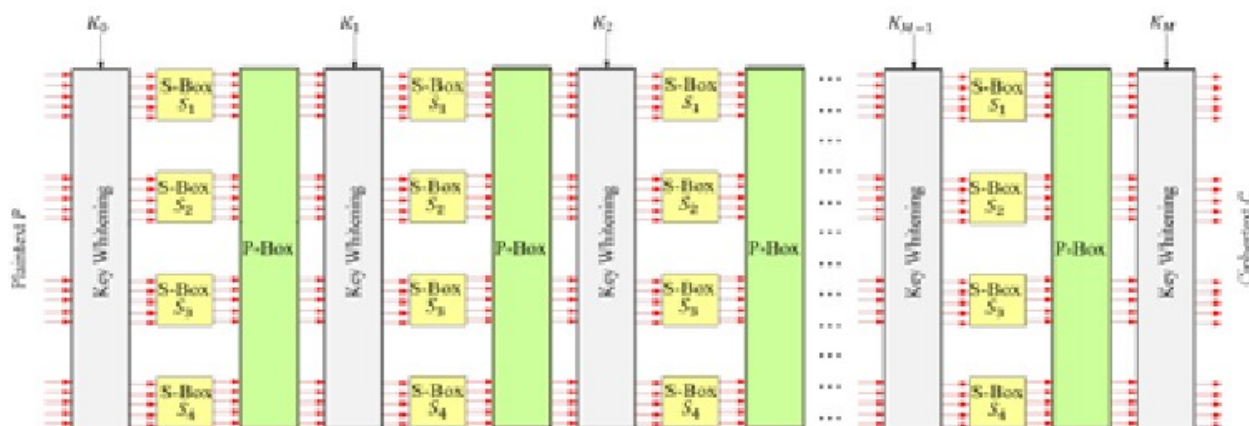


Fig. 2. Substitution-Permutation Network.

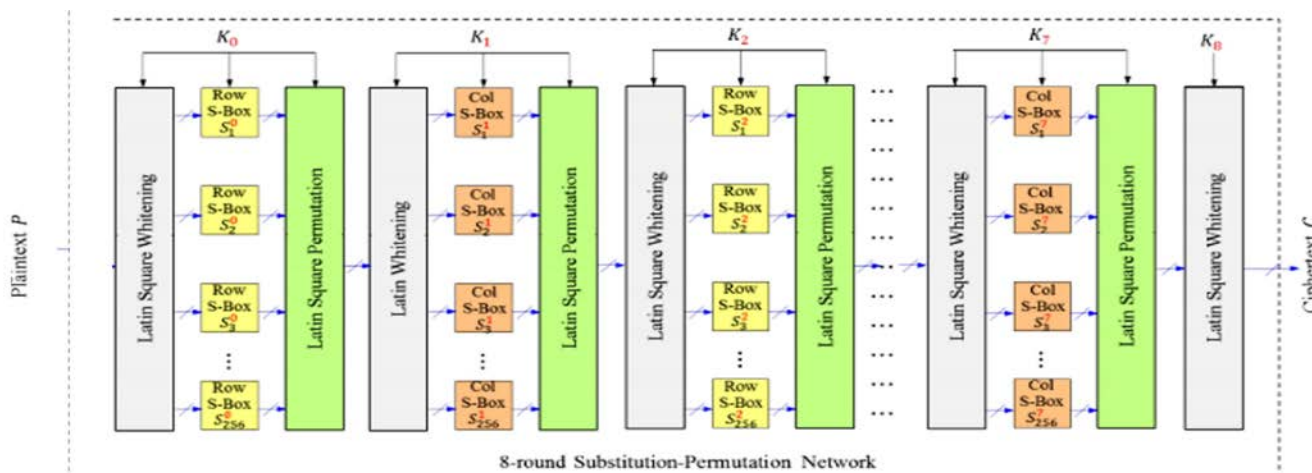


Fig. 3. Block Diagram of Latin Square Image Cipher with 8-round SPN.

### F. Latin Square Substitution

S-box is frequently applied to accomplish byte substitution in the calculation of cryptographic images. All S-Box is recognized as bijection, furthermore a definite function that can be mapped as one-to-one. In the encoding process, image pixels are associated with the image as 8-bit or byte. That is a grayscale image of 8-bit that contains intensity with a grayscale of 32-byte along with every intensity is essential of 8-bit. Normally there is a presence of forwarding row and column mapping, this forward column along with row mapping will map to Latin square. Byte replacement is achieved in image cipher by the corresponding mapping which is termed as Latin Square S-box of replacement.

$$\text{LSRS:} \begin{cases} \mathbf{C} = \text{Ecr}(\mathbf{L}, \mathbf{P}) \\ \mathbf{P} = \text{Dcr}(\mathbf{L}, \mathbf{C}) \end{cases}_{\text{ROW}}$$

LSRS function in form of a pixel in cipher image is represented in row forwarding plotting function merely by Latin Square L via a function restriction to have cipher text, similarly, IRM is the reverse function to obtain plaintext.

$$\text{ECR}_s^{\text{row}}: \\ \text{C}(r,c) = \begin{cases} \text{FRM}(\mathbf{L}, \mathbf{C}(r-1, c), \mathbf{P}(r, c)), \text{ if } r \neq 0 \\ \text{FRM}(\mathbf{L}, 0, \mathbf{P}(r, c)), \text{ if } r = 0 \end{cases}$$

$$\text{DCR}_s^{\text{row}}: \\ \text{P}(r,c) = \begin{cases} \text{IRM}(\mathbf{L}, \mathbf{C}(r-1, c), \mathbf{C}(r, c)), \text{ if } r \neq 0 \\ \text{IRM}(\mathbf{L}, 0, \mathbf{C}(r, c)), \text{ if } r = 0 \end{cases}$$

$$\text{LSCS:} \begin{cases} \mathbf{C} = \text{Ecr}(\mathbf{L}, \mathbf{P}) \\ \mathbf{P} = \text{Dcr}(\mathbf{L}, \mathbf{C}) \end{cases}_{\text{COL}}$$

Similarly, for the column pixel function of LSCS, cipher image is represented utilizing FCM function over Latin Square L to obtain ciphertext. Similarly, ICM is a reverse function to obtain the plain test and is represented as.

$$\text{ECR}_s^{\text{col}}: \\ \text{C}(r,c) = \begin{cases} \text{FCM}(\mathbf{L}, \mathbf{P}(r, c), \mathbf{C}(r, c-1)), \text{ if } c \neq 0 \\ \text{FCM}(\mathbf{L}, \mathbf{P}(r, c), 0), \text{ if } c = 0 \end{cases}$$

$$\text{DCR}_s^{\text{col}}: \\ \text{P}(r,c) = \begin{cases} \text{ICM}(\mathbf{L}, \mathbf{C}(r, c), \mathbf{C}(r, c-1)), \text{ if } c \neq 0 \\ \text{ICM}(\mathbf{L}, \mathbf{C}(r, c), 0), \text{ if } c = 0 \end{cases}$$

After implementation of Latin square substitution, input plaintext image P will have converted in an unidentifiable image, by applying LSRS and LSCR, the resultant output will be in histogram pattern.

### G. Latin Square Permutation

The permutation is mainly required to use P-box for its implementation. This P-Box is referred to as bijection, which specifies one-to-one mapping. This P box of Latin square will plot corresponding integer numbers to each row or column that permutes a series of data in integer. Latin square permutation can achieve both forward and reverse plotting for both row and column mapping function for the  $r^{\text{th}}$  row and  $c^{\text{th}}$  column respectively and represented as:

$$\begin{cases} \mathbf{y} = \text{FRM}(\mathbf{L}, \mathbf{r}, \mathbf{x}) = \mathbf{L}(\mathbf{r}, \mathbf{x}) \\ \mathbf{x} = \text{IRM}(\mathbf{L}, \mathbf{r}, \mathbf{y}) = \text{argmax}(f(\mathbf{r}, \mathbf{z}, \mathbf{y})) \end{cases}$$

$$\begin{cases} \mathbf{y} = \text{FCM}(\mathbf{L}, \mathbf{x}, \mathbf{c}) = \mathbf{L}(\mathbf{x}, \mathbf{c}) \\ \mathbf{x} = \text{ICM}(\mathbf{L}, \mathbf{y}, \mathbf{C}) = \text{argmax}(f(\mathbf{r}, \mathbf{c}, \mathbf{y})) \end{cases}$$

where x and y, represent input and output relating to plotting function, respectively.

## IV. RESULT AND DISCUSSION

Implementation of this work for Encryption as well as Decryption was using MATLAB R2014a, results were simulated and are explained as provided. The results have been divided into four parts as shown below.

### A. Encryption and Decryption for 8 Round Grayscale Image

Encryption of grayscale Latin Square Cipher image block for 8 rounds, requires a 32-byte K key, 32\*32 bytes, 1byte image block (grayscale) for P to determine C that is of 32\*32 byte of grayscale with 1 byte of the block, Fig. 4 represents a Latin square grayscale cipher image block for 8 rounds of encryption.

Similarly, for 8 rounds of decryption value P is determined for the grayscale 1 byte of 32\*32 bytes by utilizing the key (K) and Cipher images (C) that is of 32-byte key and grayscale of 1 byte of 32\*32 byte. Decryption for 8 round grayscale cipher image using Latin Square is as shown in Fig. 5. For this purpose ship image available in MatLab is utilized for encryption as well as decryption.

### B. Encryption and Decryption for 4 Round Grayscale Image

Encryption of grayscale Latin Square Cipher image block for 4 rounds, requires a 32-byte K key, 32\*32 bytes, 1byte image block (grayscale) for P to determine C that is of 32\*32 byte of grayscale with 1 byte of a block, Fig. 6 represents a Latin square grayscale cipher image block for 4 rounds of encryption.

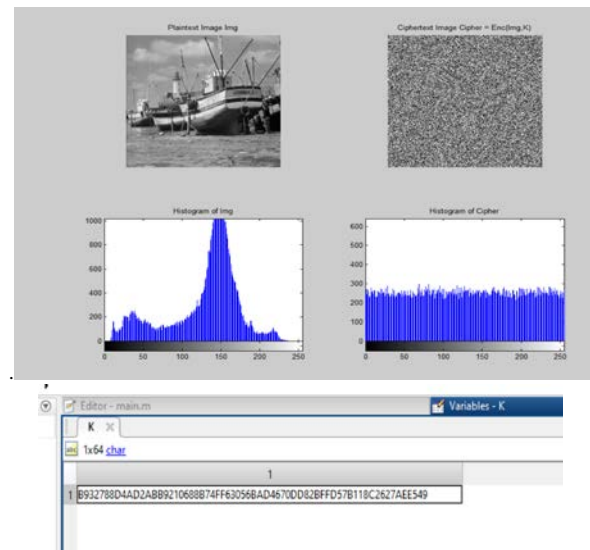


Fig. 4. Encryption of Latin Square Grayscale Cipher Block Image after 8 Rounds.



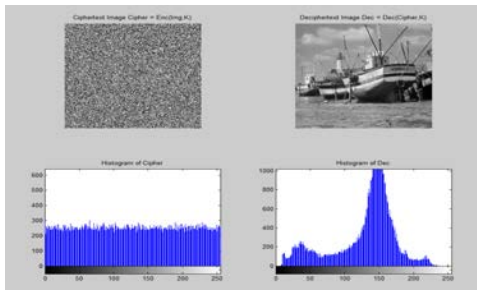


Fig. 5. The Decryption of Latin Square Grayscale Cipher Image after 8 Rounds.

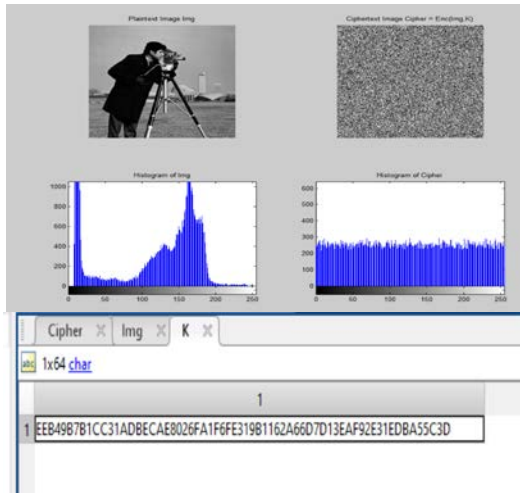


Fig. 6. Latin Square Grayscale Image Cipher block- Encryption for 4 Rounds.

Similarly, for 8 rounds of decryption value P is determined for the grayscale 1 byte of  $32 \times 32$  bytes by utilizing the key (K) and Cipher images (C) that is of 32-byte key and grayscale of 1 byte of  $32 \times 32$  byte. Decryption for 8 round grayscale cipher image using Latin Square is as shown in Fig. 7. For this purpose, in internet-based cameramen image utilized that is available in Mat lab for both encryptions as well as decryption.

### C. Latin Cube Color Image Cipher block- Encryption and Decryption

Encryption and decryption of grayscale Latin cube color Cipher image require a 32-bit K key,  $32 \times 32$  bytes, image block (color) for P to determine C and for decryption, it is to find back P image with Key K, Fig. 8 represents a Latin cube color cipher image block for both encryption as well as decryption.

### D. Key Change Analysis

1) Encryption and decryption process for Latin Square Grayscale Image Cipher block with the same key (8 rounds): Encryption of grayscale Latin Square Cipher image block for 8 rounds, requires a K key, plain text image P to determine C. For decryption P is determined with the same key and C block, Fig. 9 represents Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds. After

applying the same key for encryption and decryption with the same K (32 bytes) the resultant image is obtained and is as shown. Fig. 10 represents Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds (when a key is same). So the distortion at receive is minimum when data is retrieved.

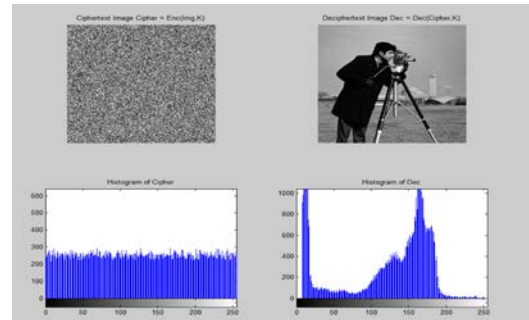


Fig. 7. Latin Square Grayscale Image Cipher for block- Decryption for 4 Rounds.

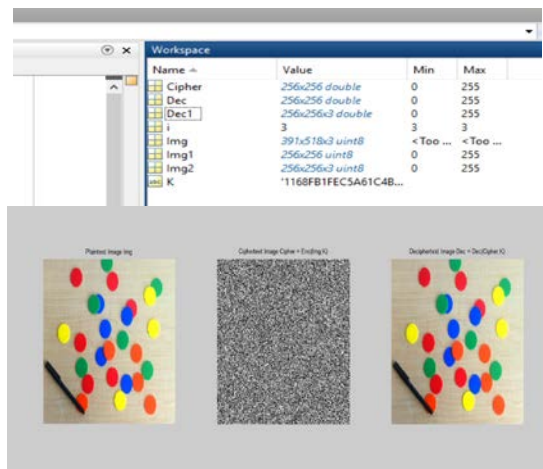


Fig. 8. Latin Cube Color Image Cipher block- Encryption and Decryption.

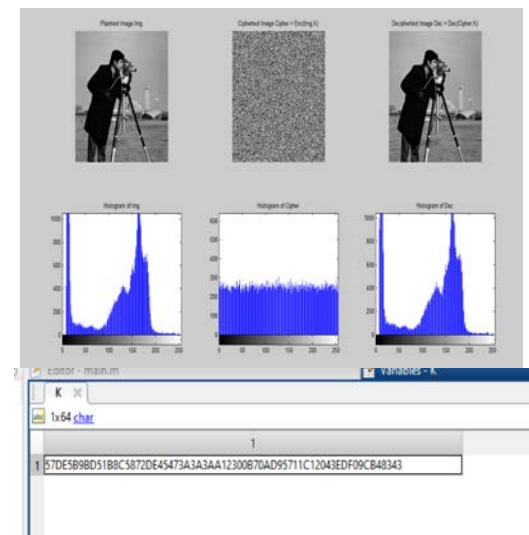


Fig. 9. Latin Square Grayscale Image Cipher Block- Encryption and Decryption for 8 Rounds.

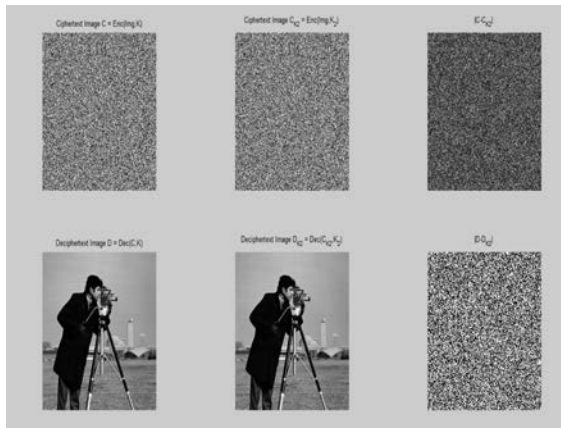


Fig. 10. Latin Square Grayscale Image Cipher Block- Encryption and Decryption for 8 Rounds (When a Key is same).

2) *Encryption and decryption process for Latin Square Grayscale Image Cipher block with a different key (8 rounds):* For encryption K1 key is required that is of 32 bytes, it is used to determine the value of C that is of size 32\*32 bytes by using the cipher image P of size 32\* 32 bytes. Similarly, in the decryption stage the value of plain text P employing cipher image C and different key K2, the result is as shown in the diagram. Fig. 11 shows different keys used for encryption and decryption for Latin Square Grayscale Cipher image for 8 rounds. The results can be compared with the images decryption with the same as well as different keys. The images obtained from different key has shown that is similar salt and pepper noise, which shows that the image that has been decrypted is unrecognizable when compared to that of decryption using the same key. The image decryption obtained from the same key has shown a better result when compared to that of a different key.

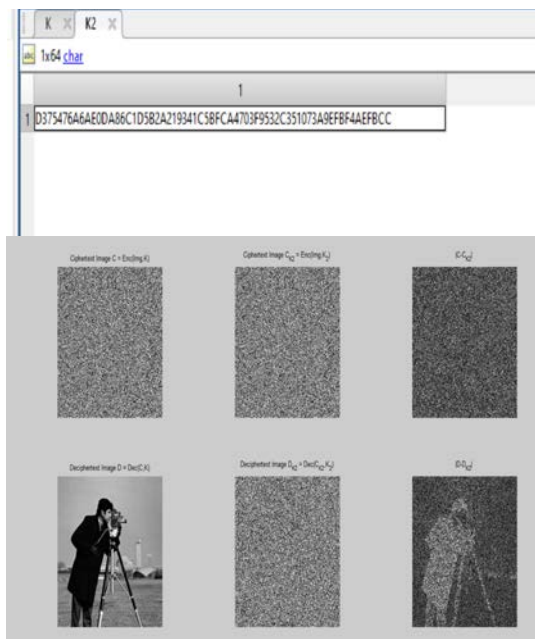


Fig. 11. Different Keys were used for Encryption and Decryption for Latin Square Grayscale Cipher Image for 8 Rounds.

The result can be tabulated as shown in the comparison table. Table I represents the difference between the plain images and decipher images after decryption image, where decipher images have shown a better result when compared to the normal decipher images. Table II shows the comparison between the present work as well as the base paper for both correlation and entropy are better when compared to the results [1].

TABLE I. COMPARISON RESULTS

Features	Plain image	Decipher image
Contrast	0.587162	0
Correlation	0.922726	Nan
Energy	0.18037	1
Homogeneity	0.8952	1
Mean	118.73	118.73
Standard deviation	62.44	62.35
Entropy	7.009	0

TABLE II. COMPARISON WITH BASE PAPER

Feature	Base paper	Proposed result
Correlation	0.9227	0.9315
Entropy	7.997	7.0097

## V. CONCLUSION

In this work, a unique image is constructed that is cipher based on Latin square as well as Latin cube. By using a grayscale image of Latin square plaintext P of 32\*32 bytes is encrypted using key K to obtain cipher images of size 32\*32, with histogram where Latin square is n\*n 2 dimensional attribute. Implementation of Latin cube for the color image is implemented using P and K key, the color image has shown better performance for the Latin cube that has a 3-dimensional attribute. The results obtained are compared with the implementation of the paper by Xu [1] has shown a better performance both in correlation as well as entropy. By using the different keys of the image is decrypted the results have shown a salt and pepper image that cannot be recognized as the original image. Simulation results have shown that the developed algorithm will preserve better security as well as advanced efficiency appropriate for real-world application. LSIC analysis has shown that Latin cube and Square in the cryptographic application have a better safety portion in terms of security as well as privacy from hackers with the change in key. Experimental security analysis with comparison between the plain image as well as decipher image is shown in the table. The distinction between plain image and decode image for the same key was 0.0037%. This result shows same data has been transmitted to the receiver to ensure that data is integrated, without loss of any information sent by the transmitter

## REFERENCES

- [1] M. Xu and Z. Tian, "An Image Cipher Based on Latin Cubes," Third International Conference on Information and Computer Technologies, pp. 160-168, DOI: 10.1109/ICICT50521.2020.00033, 2020.

- [2] Belazi, Akram, Ahmed A. Abd El-Latif, Safya Belghith. "A novel image encryption scheme based on substitution-permutation network and chaos", *Signal Processing*, pp 155-170, 2016.
- [3] Chen, Guanrong, Yaobin Mao, Charles K. Chui. "Asymmetric image encryption scheme based on 3D chaotic cat maps", *Chaos, Solitons & Fractals*, pp 749-761, 2004.
- [4] Zhang, Yong, Yingjun Tang. "A plaintext-related image encryption algorithm based on chaos", *Multimedia Tools and Applications*, pp 6647-6669, 2016.
- [5] Wang Bo, F Zou, Jun Cheng, "A memristor-based chaotic system and its application in image encryption", *Optick*, pp 538-544, February 2018.
- [6] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001, DOI: 10.1109/7384.963463.
- [7] Robert Matthews, "On the derivation of a chaotic encryption algorithm", *Cryptologia*, pp29-42, Vol 13, 1989.
- [8] Yue Wu, Yicong Zhou, Joseph P. Noonan and Sos Agaian. "Design of image cipher using Latin squares", *Information Sciences*, p 317-339, 2014.
- [9] Machkour, M., A. Saaidi, M. L. Benmaati. "A novel image encryption algorithm based on the 2-dimensional logistic map and the Latin square image cipher", *3D Research*, pp1-18, 2014.
- [10] Nema and Tanvi. "A Symmetric-Key Latin Square Image Cipher with Probabilistic Encryption for Grayscale and Color Images", *IJCSIT, International Journal of Computer Science and Information Technologies*, Vol. 8 (3), pp 380-388, 2017.
- [11] Chai, Xiuli, et al. "Medical image encryption algorithm based on Latin square and memristive chaotic system." *Multimedia Tools and Applications* pp 35419-35453, 2019.
- [12] M. Lin, F. Long and L. Guo, "Grayscale image encryption based on Latin square and cellular neural network," *Chinese Control and Decision Conference*, pp. 2787-2793, DOI: 10.1109/CCDC.2016.7531456, 2016.
- [13] S. K. N. Kumar, H. S. S. Kumar and H. T. Panduranga, "Hardware-software co-simulation of dual image encryption using Latin square image," *Fourth International Conference on Computing, Communications and Networking Technologies*, pp. 1-5, DOI: 10.1109/ICCCNT.2013.6726681, 2013.
- [14] S. Chapaneri and R. Chapaneri, "Chaos-based image encryption using Latin rectangle scrambling," *Annual IEEE India Conference*, p. 1-6, DOI: 10.1109/INDICON.2014.7030358, 2014.
- [15] Jude Hemanth and S. Smys *Computational Vision and Bio-Inspired Computing*, Springer Science and Business Media, Lecture Notes in computational vision and biomechanics, vol 28, 2018
- [16] Xu, M. and Tian, Z, "An Image Cipher Based on Latin Cubes." *Third International Conference on Information and Computer Technologies*, pp. 160-168. March 2020.
- [17] Hua, Z., Li, J., Chen, Y, Yi, S, "Design and application of an S-box using complete Latin square". *Nonlinear Dynamics*, 104(1), pp.807-825, 2021.
- [18] Khalid, S. S. Jamal, T. Shah, D. Shah and M. M. Hazzazi, "A Novel Scheme of Image Encryption Based on Elliptic Curves Isomorphism and Substitution Boxes," in *IEEE Access*, vol. 9, pp. 77798-77810, 2021, DOI: 10.1109/ACCESS.2021.3083151.
- [19] Zhongyun Hua, Jiaxin Li, Yongyong Chen and Shuang Yi. "Design and application of an S-box using complete Latin square", *Nonlinear Dynamics* Vol 104, pp 807-825, 2021.
- [20] H. Mou, X. Li, G. Li, D. Lu and R. Zhang, "A Self-Adaptive and Dynamic Image Encryption Based on Latin Square and High-Dimensional Chaotic System," *Third International Conference on Image, Vision and Computing*, pp. 684-690, DOI: 10.1109/ICIVC.2018.8492876, 2018.
- [21] Subjajith Adhikari and Sunil Karfoma, "A Novel image encryption method for e-governance application using elliptic curve pseudo-random number and chaotic random number sequence", *Multimedia Tools and Applications*, Springer series 2021.
- [22] Ashish S. Dongare, Dr. A. S. Alvi, N. M. Tarbani, "An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application", *International Research Journal of Engineering and Technology*, Volume: 04, Issue: 04, 2017.