Design of secure Image Cipher for Cryptographic Applications.

VINAYA DHAVALAGI
Electronics and Communication
Ramaiah Institute of Technology
(Autonomous Institute, Affiliated to VTU)
Accredited by National Board of Accreditation & NAAC with ‘A^{+}’ Grade
MSR Nagar, MSRIT Post, Bangalore-560054
INDIA

Abstract: - The main focus of our project is an image encryption based on substitution and permutation using Latin square and Latin cube image cipher for grayscale image and color image. The proposed methodology, Latin square image encryption mainly consists of Latin square whitening, Latin square S-box and Latin square P-box. Considering the privacy and confidentiality in the present era, securing certain stored data and the communication from theft and misuse has major concern. So a suitable methodology has been implemented for securing communicated and stored data by using a cryptographic techniques. Cryptography is the study of mathematical techniques which is related to the information security such as data integrity, confidentiality, and entity authentication and data origin authentication. The message will be in the form of plaintext image. The process of converting this plaintext image into unrecognizable is known as encryption. An encrypted message is known as ciphertext image. The process of getting back the Ciphertext is known as decryption. As security is a major concern in storing of images and communication. Image encryption has wide range of applications in internet communication, medical imaging, military affairs and many more.

Key-Words: - Decryption, Encryption, Latin Square Generator, Sequence Generator.

1 Introduction

With the rapid requirement of transmitting the multimedia information through internet and network, many communication techniques are developed with the peace of mind that the protection of the info has not been compromised. Security of data plays a vital role in every aspect of life [11]. For keeping the knowledge secure, goals of security CIA (confidentiality, Integrity, and Availability) should be achieved like confidentiality where information is kept a secret from an unauthorized source, integrity where information is kept unchanged by unauthorized source, availability where only authorized people to possess access to the knowledge the opposite important security goal is authentication where the identity of an entity is validated and preserved[11]. Implementing these goals not only on the stored information but also when the information is transmitted or exchanged with the employment of the web is challenging. The information is misused if the protection of sensitive information is breached. Cryptographic methods or tools are accustomed ensure all the goals of security. Cryptography is used to provide different security services within the electronic world[1]. It is the easiest way of transforming a message into another unintelligent form which isn't understandable by an unauthorized person with an aim to make it immune to attacks. It involves different mechanisms like symmetric key, asymmetric key encipherment. Symmetric and asymmetric key encipherment are the algorithms that are used to perform encryption and decryption on data which is analogous to electronic locking of knowledge [9]. The first method uses one secret or private key that's being shared between sender and receiver for performing encryption and decryption. The other technique is using general public and private key combine where the best public key wont in order to encode the data as well as a private key accustomed decode that the data. Latter is safer because it doesn't face any problem of key distribution as within the case of symmetric schemes. But it's longer consuming because it requires high mathematical computations. Both these techniques exist in parallel and still serve the community. they're complements of every other; the advantage of one can atone for the disadvantage of the opposite. Encryption and decryption are referred as ciphers/algorithms.

In symmetric or asymmetric encipherment, the plaintext P also called secret information is transformed into ciphertext C through any of the encryption algorithm [11]. The information is not always transmitted in secured channel. The main goal here is to maintain the confidentiality that is the information should not be revealed to an unauthorized person without the knowledge of correct keys. In the cryptanalysis, according to Kirchhoff's principle, it is always assumed that encryption algorithm and other resources such as plaintext-ciphertext pair are already understood to the attackers. Therefore, the level of resistance of the cipher should make depending upon the privacy of the key. Such that private key used must be strong enough so that attacker should not be able to break it or cryptanalyze it. For this purpose, the key domain for an image encryption algorithm should be large enough that it becomes immune to brute force or exhaustive search attack[1][9][11].

2 Background

As there is a rapid growth in technology, the digital images are very important in people day to day life. Under this condition image encryption has become very important. Image encryption provides a security for the images by converting the original images to unrecognizable one[9]. The main importance of image encryption is used in medical treatment e-commerce, military applications and many more [11].

These days, comparing with general text information, digital and secure images have various immense characters such as wide content, maximum info repetitiveness and a extremely powerful correlativity in between each nearby pixels [1]. According many encryption algorithms have been purposed on images, but an existing encryption algorithm has occupied its own important position.

2.1 Objective of Project

In digital world, cryptography offers three core area which protect you along with your data from unauthorized users, from attempt of theft. The main goals of cryptography are to provide confidentiality, authenticity and integrity.

2.1.1 Data privacy also known as confidentiality which means that the particular information is actually hidden by encrypting it. Transmitter encrypts that information via private key. Receiver decrypts that information using same private key used at encryption.

2.1.2 Data authenticity is to guarantee that a person or a method can be their identification to another would you not have knowledge this is certainly personal of identification.

2.1.3 Data integrity is to ensure that the data received is same as that of data which is sent by the sender. Integrity is mainly assurance that any piece of information has not been altered.

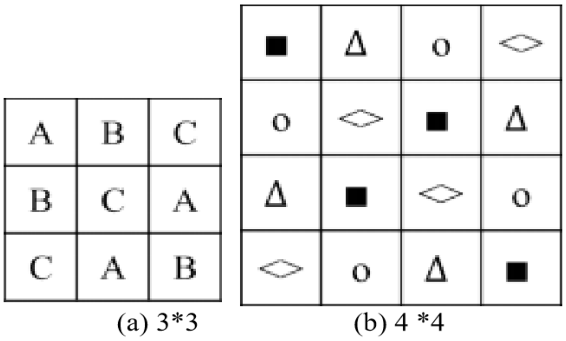
3 Methodology

Considerations of privacy and confidentiality in this generation have given recognition to the necessity for securing certain communications and stored data from theft and misuse [11]. An appropriate methodology for securing communicated or stored data involves the utilization of cryptographic techniques. Cryptography is that the study of mathematical techniques related with features of information protection like privacy, data reliability, and entity authentication and data source authentication [11][9]. An information is plain text. The technique concerning hiding your message as part of this type of exactly the ways in order to protect the matter is actually encoding. The encode content is actually encode content. The methodology of transforming cipher content immediately previously to plain content is actually deciphering.

The domain of encryption is turning into important inside the present era during the course of which data safety is actually a of extreme issue. Safety is actually a important issue as part of communications as well as storage of images, and also encryption is actually an individual among the the ways towards make certain security [8]. Image encoding includes a huge number of applications as part of internet communication, health-related imaging like reviewed report, telemedicine, military services affairs, and so on. Encrypting plaintext leads to incomprehensible trash called cipher content. Encryption is employed towards ensure the hidden information from anyone of concern not meant in order to, additionally those which can comprehend that the encoded data. The process of backsliding cipher text to its authentic plaintext is referred as decryption.

3.1 Latin Square

A Latin square (N) is a particular N *N assortment filled as with a symbol set of N distinctive elements, with every symbol appears correctly once in each row and each column [11]. The label Latin Square is inspired by the mathematician Leonhard Euler, who used Latin characters as symbols.



A	B	C
B	C	A
C	A	B

(a) 3*3

■	Δ	o	◇
o	◇	■	Δ
Δ	■	◇	o
◇	o	Δ	■

(b) 4 *4

Fig.1 Example of Latin Square with different order and different symbol set.

3.2 Latin Square Generator

Latin square of order N is generated from the two sequences of same length. Let QUAN1 as well as QUAN2 are two length-N sequences [11].

Latin square generator L=LSG(QUAN1, QUAN2)

Require: - QUAN1 and QUAN2 are two length-N sequences

Ensure: - L is a Latin square of order N

```
QA = SortMap(QUAN1)

QB = SortMap(QUAN2)

For r=0 to N-1

L(r, : )=Rowshift(QA, QB(r))

End
```

The only two sequences QUAN1 and QUAN2 are generally designed by a pseudo-random number generator(PRNG).SortMap(QA,QB) is a function which identifies the index in between a QA &QB series and also it is altered edition QA* as part of the acclivitous order, and Row Shift operation is done (QA, v) that will make a periodic transfer of the QA pattern with v elements to the left[10][11][9].

3.3 Substitution-Permutation Network.

As part of cryptography, an input message is actually known to as plaintext as well as an output message is referred as a ciphertext [1]. A permutation substitution network is a cipher design which is mostly comprised of a number regarding substitution and permutation ciphers with numerous iterations. This substitution and permutation system design is used in numerous a variety of algorithms known block ciphers, for example. Rijndael i.e.AES [8][9][11].

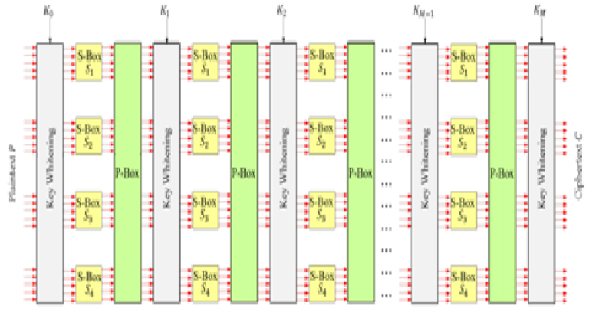


Fig.3.3 A M-round substitution-permutation network for block ciphers.

During the N-round Permutation and substitution network, a plaintext which in turn is actually in bit series and represented with a symbol P, is actually the initial and source content which one is need to be encoded. Ciphertext is the output bit series C, is actually the encoded content through substitution and permutation network [11].A Substitution and permutation network stage that contain three file encoding primitives: -

- Latin Square Whitening.
- Latin Square Substitution.
- Latin Square Permutation.

Latin square whitening is generally an operation to constantly mix the plaintext with a round key. Latin Square Substitution is to map one input byte to another byte. Latin Square Permutation is actually a shuffling bit location with the input bit series[8].The decryption process of a substitution and permutation network cipher is as similar as to reverse the process that is to perform inverse Latin Square Permutation Substitution [11][8].

3.4 Latin Square Image Cipher

For encoding/ decoding process that the cipher handling block is set seeing while 256*256 grayscale segment, and its actual pixel intensity level is actually arranged to1 byte. Here, we utilise P to describe a (32*32)byte plain text image section, C to represent (32*32)byte Cipher image block of P. L to describe Latin Square (32 byte), and K to represent (32 byte) encryption key. The recommended Latin square image cipher is actually involving the substitution and permutation network structure which carries out 4 rounds and also 8 rounds [9][11].

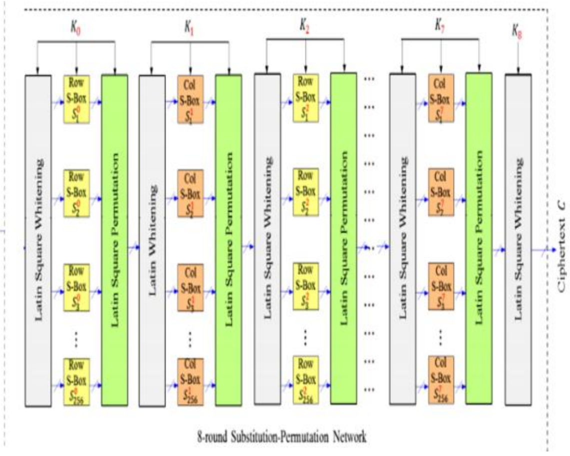


Fig.3.4 Block Diagram of Latin square image Cipher with 8-round SPN.

3.5 Latin Square Whitening

A part of the standard SPN technique for the section ciphers, the Whitening phase means that generally mixes a plaintext content P along with the round key.i.e, to perform XOR process. As part of image encoding, an image block is actually included as an plaintext content P, composed of 8-bit pixels [11]. As part of conventional method XOR whitening method become unacceptable as well as ineffective for the image information.

As the main goal concerning whitening is actually in order to mix plain content with the sequence keys, so we complete rearrangement cipher through Finite field/Galois field(2^8) for plain image, equation is actually as presented in below

$$y = [x + l] 2^8 \qquad (1)$$

This particular above Latin square whitening procedure can easily be easily reversed, as determined in the just below equation,

$$x = [y + l]2^8 \qquad (2)$$

Where y is the whitening result in byte.

l is the Latin square in byte.

x is plain text image in byte.

2^8 denotes the calculation over finite field/Galois field.

In image encryption, the pixel level equation is depicted as follows

$$C(r, c) = [SR(P(r, c),[D]3)+L(r, c)]\ 2^8 \qquad (3)$$

$$P(r, c) = SR([C(r, c)+L(r, c)]\ 2^8, [D]3) \qquad (4)$$

Here, P is actually plain text and x is a pixel(8 bit), positioned as of rth row and cth column P(r, c). L is Latin square element positioned as of rth row and cth column L(r, c). D is referred to as rotating factor, and SR is actually spatial rotating function(X, d) where it revolves X image corresponding to the a variety of values of d which is actually as explained below

Y=SR(X, d)={¦(X, if d=0

Flip X up/down, if d=1

Flip X left/right, if d=2)} (5)

Applying Latin square key whitening to all pixel level, subsequently an image can be represented as

LSW : {¦(C=Ecr(L,P,D)

P=Dcr(L,C,D))} (6)

Where LSW is Latin Square Whitening [1][11].

3.6 Latin Square Substitution.

As part of cryptography, a S-box is mostly applied in order to perform byte substitution. Every single S-Box is identified as bijection, additionally defined to be one-to-one map function. As image encoding, pixel related with image is symbolized as 8-bit, the byte. For the example, grayscale image of 8-bit that includes 256 grayscale intensity as well as each intensity is actually of 8-bit.As generally there is actually an existence out of forward row/column mapping and Forward column/row mapping onto mapping in Latin square, We can perform byte replacement using one-to-one mapping in a image cipher and this form of replacement is actually termed as Latin square S-box[9][11]. In the substitution with relation to a row is termed as Latin Square Row S-box(LSRS) as follows

$$\text{LSRS}:\begin{cases}\mathrm{C}=\mathrm{Ecr}(\mathrm{L},\mathrm{P})\\ \mathrm{P}=\mathrm{Dcr}(\mathrm{L},\mathrm{C})\end{cases}_{\text{ROW}} \qquad (7)$$

As part of pixel-level function of LSRS, cipher text is actually depicted in Forward row mapping function simply by Latin square L using a function parameters in order to have ciphertext to reverse and to get plaintext we use IRM the equations as

$$\mathrm{ECR}_s^{row}:\mathrm{C(r,c)}= \begin{cases}FRM\big(L, C(r-1,c), P(r,c)\big), if\ r\neq 0\\ FRM\big(L,0,P(r,c)\big), if\ r=0\end{cases} \qquad (8)$$

DCR_s^{row}:

$$\mathrm{P(r,\ c)}=\begin{cases}IRM\big(L, C(r-1,c), C(r,c)\big), if\ r\neq 0\\ IRM\big(L,0,C(r,c)\big), if\ r=0\end{cases} \qquad (9)$$

In the substitution with relation to a column is termed as Latin Square Column S-box(LSRS).

$$\text{LSCS}:\begin{cases}\mathrm{C}=\mathrm{Ecr}(\mathrm{L},\mathrm{P})\\ \mathrm{P}=\mathrm{Dcr}(\mathrm{L},\mathrm{C})\end{cases}_{\text{COL}} \qquad (10)$$

As part of pixel-level function of LSCS, ciphertext is actually depicted by just FCM function through Latin square L with a function variables in order to get ciphertext to invert as well as in order to have plaintext we use ICM the equations as follows

$$\mathrm{ECR}_s^{col}:\mathrm{C(r,c)}= \begin{cases}FCM\big(L, P(r,c), C(r,c-1)\big), if\ c\neq 0\\ FCM(L,P(r,c),0), if\ c=0\end{cases} \qquad (11)$$

$$\mathrm{DCR}_s^{col}:\mathrm{P(r,c)}= \begin{cases}ICM\big(L, C(r,c), C(r,c-1)\big), if\ c\neq 0\\ ICM(L,C(r,c),0), if\ c=0\end{cases} \qquad (12)$$

Immediately after applying Latin square substitution their plaintext image P will certainly become unrecognizable just after performing LSRS as well as LSCR, what can become noticed in histogram analysis[1][8][11].

3.7 Latin Square Permutation.

In cryptography, a P-box is mainly used to perform byte permutation. Each P-Box is known as bijection, also defined as one-to-one mapping. Within Latin square P-box, map that the integer number series to whichever row or even column, which permutes series out of integer data.

In Latin square permutation we can easily able to design Forward and inverse row mapping and column mapping function to the rth row as well as cth column correspondingly as shown in the equations

$$\begin{Bmatrix} y = FRM(L,r,x) = L(r,x)\\ x = IRM(L,r,y) = argmax(f(r,z,y))\end{Bmatrix} \quad (13)$$

$$\begin{Bmatrix} y = FCM(L,x,c) = L(x,c)\\ x = ICM(L,y,C) = argmax(f(r,c,y))\end{Bmatrix} \quad (14)$$

Exactly where x as well as y describe that the input and the output concerning the map functionality respectively [1][11][9].

3.8 Results and Discussion

Encryption and Decryption: - MATLAB R2014a

3.8.1 Simulation Results

Latin Square Grayscale Image Cipher block-

- **Encryption for 8 Rounds.**
- Needed: K is a 32 byte key.
- Needed: P is a (32*32) byte, 1-byte grayscale image block.
- Determine: C is a (32*32) byte, 1-byte grayscale image block.

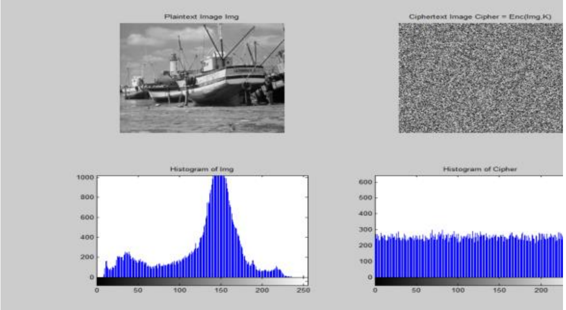
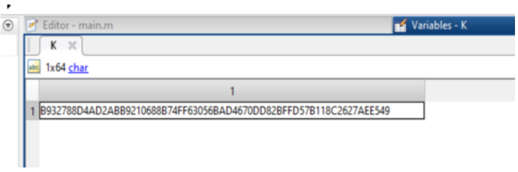


Figure 3.8.1 *a)Latin Square Grayscale Image Cipher block- Encryption for 8 Rounds.*

3.8.2 b) Simulation Results.

- **Decryption for 8 Rounds**
- Needed: K is a 32-byte key.



1 B932788D4AD2ABB9210688B74FF63056BAD4670DD82BFFD57B118C2627AEE549

- Needed: C is a (32*32) byte, 1-byte grayscale image block.
- Determine: P is a (32*32) byte, 1-byte grayscale image block.

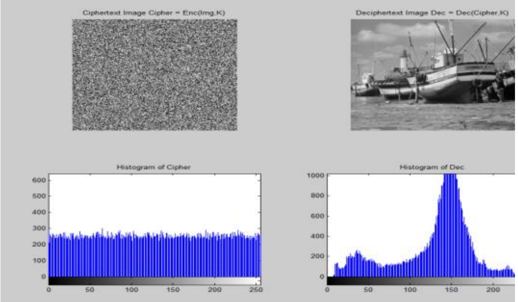


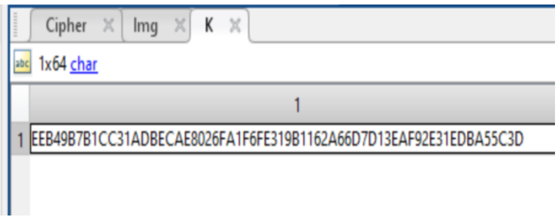
Figure 3.8.2 b)Latin Square Grayscale Image Cipher block- Decryption for 8 Rounds.

3.8.3 a) Simulation Results

Latin Square Grayscale Image Cipher block

Encryption for 4 Rounds.

- Needed: K is a 32-byte key.



1 EEB49B7B1CC31ADBECAE8026FA1F6FE319B1162A66D7D13EAF92E31EDBA55C3D

- Needed: P is a (32*32) byte, 1-byte grayscale image block.
- Determine: C is a (32*32) byte, 1-byte grayscale image block.

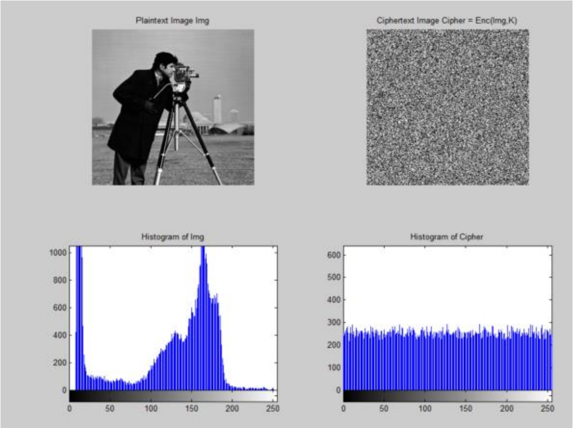
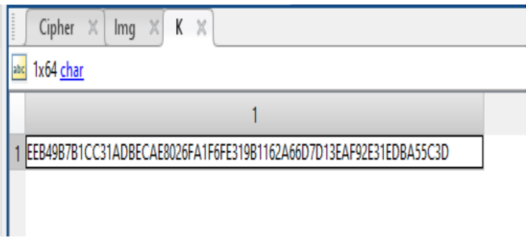


Figure 3.8.3 a)Latin Square Grayscale Image Cipher block- Encryption for 4 Rounds.

3.8.4 b) Simulation Results

Decryption for 4 Rounds

- Needed: K is a 32-byte key.



1 EEB49B7B1CC31ADBECAE8026FA1F6FE319B1162A66D7D13EAF92E31EDBA55C3D

- Needed: C is a (32*32) byte, 1-byte grayscale image block.
- Determine: P is a (32*32) byte, 1-byte grayscale image block.

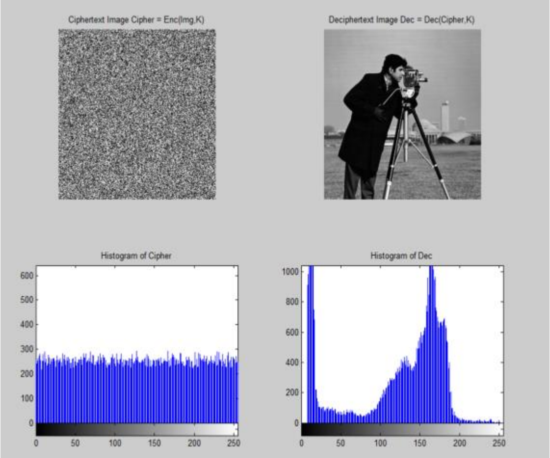
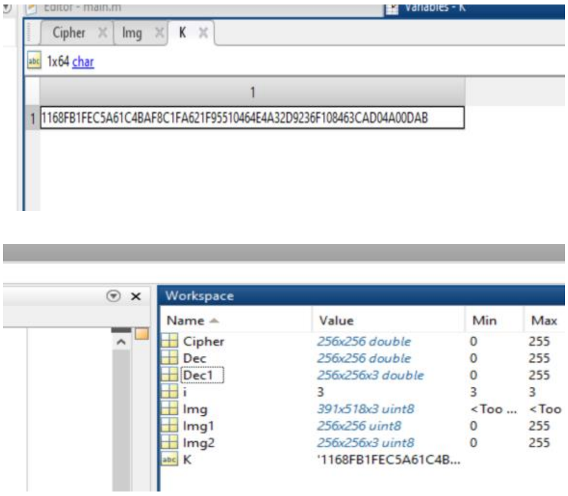


Figure 3.8.4 b) Latin Square Grayscale Image Cipher for block- Decryption for 4 Rounds.

4.3 Simulation Results

Latin Cube Color Image Cipher block- Encryption and Decryption

- ➢ Needed: K is a 32-byte key.



1 1168FB1FEC5A61C4BAF8C1FA621F95510464E4A32D9236F108463CAD04A00DAB

Workspace

Name	Value	Min	Max
Cipher	256x256 double	0	255
Dec	256x256 double	0	255
Dec1	256x256x3 double	0	255
i	3	3	3
Img	391x518x3 uint8	<Too ...	<Too
Img1	256x256 uint8	0	255
Img2	256x256x3 uint8	0	255
K	'1168FB1FEC5A61C4B...		

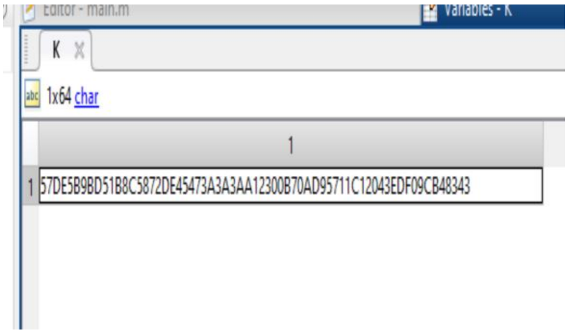
Figure 3.8.4 Latin Cube Color Image Cipher block- Encryption and Decryption.

3.8.5 a) Simulation Results

Key Change Analysis: -

Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds(when key is same)

- ➢ Needed: K is a 32-byte key.



1 57DE5B9BD51B8C5872DE45473A3A3AA12300B70AD95711C12043EDF09CB48343

- ➢ Needed: C is a (32*32) byte, 1-byte grayscale image block.

- ➢ Determine: P is a (32*32) byte, 1-byte grayscale image block.

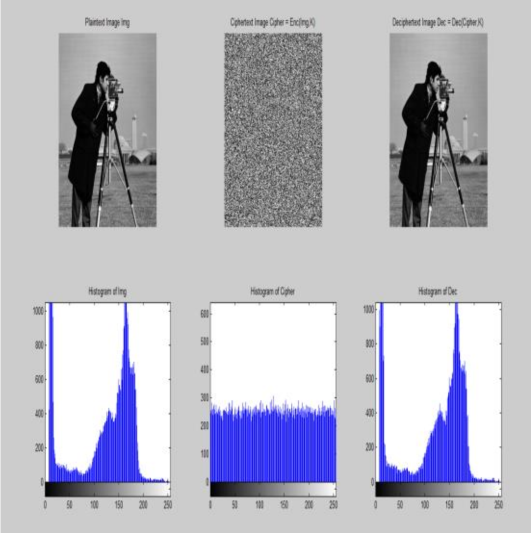
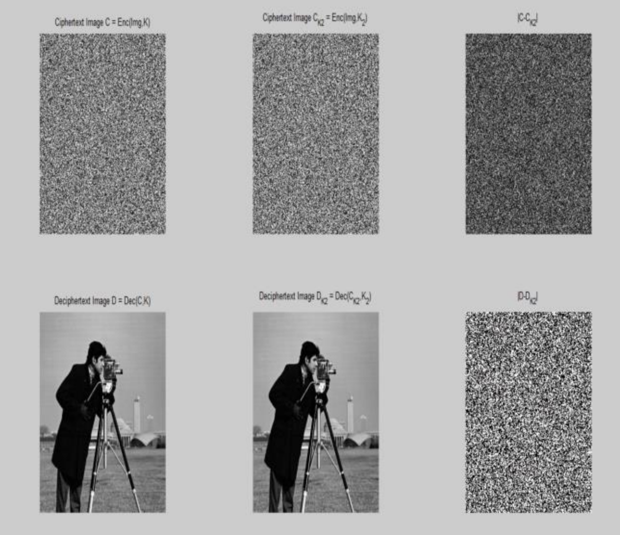


Figure 3.8.5 a) Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds

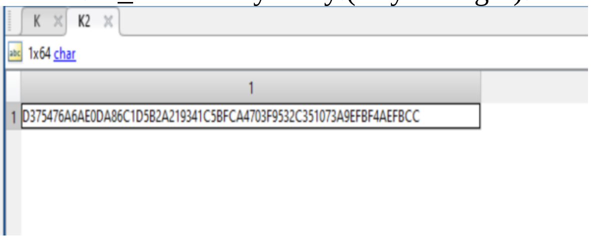


Ciphertext Image C = Enc(Img,K)
Ciphertext Image C_{K2} = Enc(Img,K_2)
|C-C_{K2}|
Deciphertext Image D = Dec(C,K)
Deciphertext Image D_{K2} = Dec(C_{K2},K_2)
|D-D_{K2}|

Figure 3.8.5 b)Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds(when key is same).

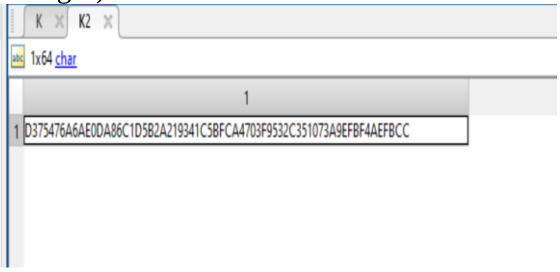
3.8.6 Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds(when key is different)

Needed: K_2 is a 32 byte key.(Key Changes).



1 D375476A6AE0DA86C1D5B2A219341C5BFCA4703F9532C351073A9EFBF4AEFBCC

- Needed: C is a (32*32) byte, 1-byte grayscale image block.
- Determine: P is a (32*32) byte, 1-byte grayscale image block.
- Needed: K_2 is a 256-bit key.(Key Changes).



D375476A6AE0DA86C1D5B2A219341C5BFCA4703F9532C351073A9EFBF4AEFBCC

- Needed: C is a (32*32) byte, 1-byte grayscale image block.
- Determine: P is a (32*32) byte, 1-byte grayscale image block.

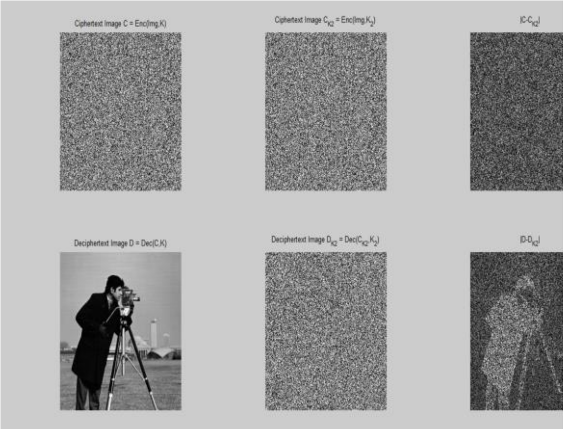
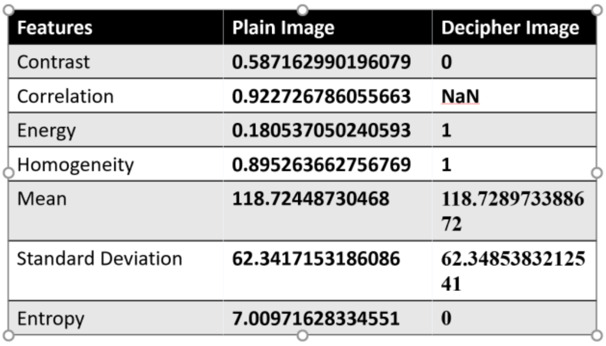


Figure 3.8.6 c) Latin Square Grayscale Image Cipher block- Encryption and Decryption for 8 Rounds(when key is different).

Comparison results



Features	Plain Image	Decipher Image
Contrast	0.587162990196079	0
Correlation	0.922726786055663	NaN
Energy	0.180537050240593	1
Homogeneity	0.895263662756769	1
Mean	118.72448730468	118.728973388672
Standard Deviation	62.3417153186086	62.3485383212541
Entropy	7.00971628334551	0

4 Conclusion

As part of this paper, we constructed the unique image cipher based on Latin square and Latin cube. Latin square on grayscale image has been implemented with histogram where Latin square is n*n 2D attribute. Additional work on Latin cube on colour image has been implemented where Latin cube is an n*n*n 3D attribute. Simulation outcomes demonstrate this particular algorithm not only includes the desired level of security, however additionally high efficiency as well as algorithm had extremely suitable for the practical application.

Merits of Latin Square and Latin Cube in cryptographic application as

- Theoretical security measures analysis reveals that LSIC has a very great level of resistance to cipher text attacks known as plain-text attacks and key change.
- Experimental security analysis with comparison between plain image as well as decipher image is shown. The distinction between plain image and decode image for same key we got 0.0037%.This design efficiently implemented in hardware.

Demerits of Latin square and Latin cube in cryptographic applications as

- In Latin square and Latin cube design, the number of rows must be equal to number of columns which is drawback we need to convert image into (256*256) pixels then can be used for encryption and decryption.
- Latin square contains, n^2 entries which may be too large.

In the future, on the basis of proposed algorithm, further research on Latin cubes in image cipher will be carried out. And the encryption schemes for videos will also be studied.

Reference

[1]. Xu, Ming, and Zihong Tian. "An Image Cipher Based on Latin Cubes." *2020 3rd International Conference on Information and Computer Technologies (ICICT)*. IEEE, 2020.

[2]. Belazi, Akram, Ahmed A. Abd El-Latif, and Safya Belghith. "A novel image encryption scheme based on substitution-permutation

network and chaos." *Signal Processing* 128 (2016): 155-170.

[3]. Chen, Guanrong, Yaobin Mao, and Charles K. Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos, Solitons & Fractals* 21.3 (2004): 749-761.

[4]. Zhang, Yong, and Yingjun Tang. "A plaintext-related image encryption algorithm based on chaos." *Multimedia Tools and Applications* 77.6 (2018): 6647-6669.

[5]. Wang, B., Zou, F. C., & Cheng, J. (2018). A memristor-based chaotic system and its application in image encryption. *Optik*, *154*, 538-544.

[6]. Kocarev, Ljupco. "Chaos-based cryptography: a brief overview." *IEEE Circuits and Systems Magazine* 1.3 (2001): 6-21.

[7]. Matthews, Robert. "On the derivation of a “chaotic” encryption algorithm." *Cryptologia* 13.1 (1989): 29-42.

[8]. Panduranga, H. T., & Kumar, S. N. (2014). Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher. *The European Physical Journal Special Topics*, *223*(8), 1663-1677.

[9]. Wu, Yue, et al. "Design of image cipher using latin squares." *Information Sciences* 264 (2014): 317-339.

[10]. Machkour, M., A. Saaidi, and M. L. Benmaati. "A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher." *3D Research* 6.4 (2015): 1-18.

[11]. Nema, Tanvi. "A Symmetric-Key Latin Square Image Cipher with Probabilistic Encryption for Grayscale and Color Images." International Journal of Computer Science and Information Technologies, Vol. 8 (3) , 2017, 380-388.

[12]. Chai, Xiuli, et al. "Medical image encryption algorithm based on Latin square and memristive chaotic system." *Multimedia Tools and Applications* 78.24 (2019): 35419-35453.

[13]. Lin M, Long F, Guo L. Grayscale image encryption based on Latin square and Cellular Neural Network. In2016 Chinese Control and Decision Conference (CCDC) 2016 May 28 (pp. 2787-2793). IEEE.

[14]. Kumar, S. N., Kumar, H. S., & Panduranga, H. T. (2013, July). Hardware software co-simulation of dual image encryption using Latin square image. In *2013 fourth international conference on computing, communications and networking technologies (ICCCNT)* (pp. 1-5). IEEE.

[15]. Chapaneri, S., & Chapaneri, R. (2014, December). Chaos based image encryption using latin rectangle scrambling. In *2014 annual IEEE India conference (INDICON)* (pp. 1-6). IEEE.

[16]. Xu, Ming, and Zihong Tian. "A novel image cipher based on 3D bit matrix and latin cubes." *Information Sciences* 478 (2019): 1-14.

[17]. Xu, M., & Tian, Z. (2020, March). An Image Cipher Based on Latin Cubes. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)* (pp. 160-168). IEEE.

[18]. Hua, Z., Li, J., Chen, Y. and Yi, S., 2021. Design and application of an S-box using complete Latin square. *Nonlinear Dynamics*, *104*(1), pp.807-825.

[19]. Hsiao, M.Y., Bossen, D.C. and Chien, R.T., 1970. Orthogonal Latin square codes. *IBM Journal of Research and Development*, *14*(4), pp.390-394.

[20]. Hua, Zhongyun, Jiaxin Li, Yongyong Chen, and Shuang Yi. "Design and application of an S-box using complete Latin square." *Nonlinear Dynamics* 104, no. 1 (2021): 807-825.