iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IV **Month of publication:** April 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Secure Sharing and Retrieval of Image in an Untrusted Cloud Environment

D. Brinda Devi[1], Dr. S. Selva Kumar[2]
Computer Science and Engineering,
GKM College of Engineering & Technology, Chennai, India

Abstract—Sharing of Medical reports and scan images of patients are helpful to take quick and perfect decisions among doctors for collaborative treatment. This will help to provide maximum care for the patients who are in long distance where the specialist doctors are not available to give treatment at the correct time. Therefore, Medical images are transmitted in the format of Digital Imaging and Communications in Medicine (DICOM) images which provides a secured communication for effective referrals among peers without affecting the privacy of patients. To provide this security for sharing of medical images, we are combining three cryptic schemes namely Latin Square Image Cipher (LSIC), Arnold Transform and Rubik's encryption as three different layers. Each encryption techniques have a unique characteristics and properties. In that, LSIC provides shuffling of the image blocks, better substitution and confusion; Arnold Transform provides randomness, erotic and sensibility and also tamper proofing; Rubik Cube basically has the property of permutation of image pixels. These algorithms are developed, implemented and tested in the MATLAB software environment. The testing can be done with various estimated metrics such as Additive White Gaussian Noise (AWGN), Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), correlation values and histograms.

Keywords—DICOM, LSIC, Arnold, Rubik's Encryption.

I. INTRODUCTION

In today's world, Security is a great challenging criteria over the network. The networking technology is in high growth which leads to a common culture for interchanging of the data very drastically. So, information has to be protected during transmission over the internet. The influence of information, communication and technology (ICT) has developed strongly in the field of medicine through tele-diagnosis, tele-consulting, and tele-surgery. Several multimedia tools are developed for sharing the e-medical data among users with high secrecy for protecting the privacy of individuals. DICOM images are mainly used for addressing the e-medical data, and it requires better and improved security than normal images. Because, DICOM image has more accountability in terms of insurance policies. It can be protected by encryption keys, digital signatures, watermarking, steganography, cryptographic algorithms, chaotic sequences and hash functions.

Security and privacy are the two most important characteristics and they have to be implemented against hackers for a secure digital communication in the present scenario. The fusion of traditional cryptic and modern chaotic features, namely confusion, diffusion, ergodicity, and randomness have evolved as a stronger tool in the form of image encryption which can be used for establishing secured digital communication.

Recently, many researchers have proposed and implemented image encryption algorithms using different transform techniques, chaotic systems, multiplexing, compression, fusion techniques and also different transform domain based image encryption algorithms, especially in gyrator domains. Additionally, Authors have adapted the Discrete Wavelet Transform (DWT), Walsh-Hadamard Transform (WHT), Binary Discrete Hartley Transform (BDHT), DCT, and hybrid diagonal block-set transform (FHDBT) techniques for image encryption applications.

To further the complexity, authors have developed image encryption algorithms based on compression techniques. Under the compression schemes, the Huffman, multiple Huffman table, run-length and dictionary algorithms were employed to generate cryptic images. During this evolution of image encryption algorithms, a novel double image scheme emerged as a multiplexed scheme. In this superimposed platform, researchers have adopted multiplexed double pixel scrambling, fractional random encoding, fractional random encoding using the chaotic approach, amplitude encoding, phase encoding and random, iterative random encoding to perform image encryption coding, also fusion algorithms were developed to encrypt both monochrome and color images.

Recently, chaotic encryption schemes plays a major role among many researchers because of their excellent randomness and complexity. A piecewise linear chaotic map was employed on a color image for scrambling, and additional confusion and diffusion

was performed simultaneously on the three color planes. In addition to linear chaotic map, the logistic, standard, tent map, skew tent map, Lorentz system, time delay Lorentz system, 6D chaotic system, Arnold cat map, circulant operations, and Tompkin's Paige algorithms were considered to perform image encryption schemes.

The transformation of pixels and matrices was performed for the secured storage and transfer of DICOM images, will be resulting in permuted, diffused and confused encrypted data. Several OpenWare tools were designed and developed to make medical images available for secondary applications including research projects and to build healthcare networks. Medical images are normally divided into two categories: region of interest (ROI) and region of background (ROB). For reducing the processing time and the number of overheads, ROI and ROB were processed separately with same or different encryption keys and algorithms. The watermarking of patient information, hospital LOGO and doctor details can be embedded on ROB while leaving ROI unchanged. To further improve authentication, the finger printing, hash functions and digital signatures of patient information were embedded as secret data on ROB.

Watermarking combined with encryption or steganography schemes and cryptographic algorithms such as AES, DES, RC4, and IDEA can be used to provide enhanced image security and authentication. To provide image protection, the efficient and real-time medical image transmission can be done by using bit level shuffling, substitution and permutation. To protect medical images, a chaotic technique, by scrambling the pixel values and by combining various cryptographic mechanisms and key management schemes.

To provide reliable, error-free transmission and reception of DICOM images, various error control codes such as repetitive and hamming codes have been used. Multiple chaotic encryption schemes with compression, watermarking and the concept of Galois field were used for enriching the security of medical data. A joint encryption and watermarking algorithm to provide a two-level security feature to medical images.

Thus, the existing techniques majorly employs either chaotic or cryptic effects, which are not enough against hackers. So, therefore, a tri-layer technique has been proposed in which confusion, diffusion, tamper proofing, permutation, randomness and ergodicity have been fused in a single platform to perform triple encryption.

The remaining paper is organized as follows. Section II discussed about proposed methodology. Section III, describes about design approach, section IV briefly explained about Proposed Algorithm, section V, discussed about image analysis and metrics, section VI, is about results and discussion, and section VII concludes with the salient features of the implemented encryption system.

II. PROPOSED METHODOLOGY

A. Latin Square Image Cipher

A Latin square matrix is an n x n matrix that consists of n different elements by which the matrix is constructed. These n elements are filled in such a way that no elements will reoccur in any row or column of the matrix, so that each row and column contains all of the elements. Leonhard Euler, a Swiss Physicist and a Mathematician proposed the concept of Latin Square image cipher (LSIC) by using Latin characters as symbols, which led to the famous Sudoku puzzle. The given 9 x 9 Latin square represents the LSIC scheme where no number repeats in a row or column, which inherently results in a confusion property suited for image encryption.

LSIC based image encryption schemes can be implemented on either hardware or software tools because of their sensitiveness to keys, suitability to bytes instead of bits and integer-based operations.

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Figure 1.1: Latin Square Image Cipher

B. Arnold Transform

1) Arnold Cat Map: Arnold cat transformation is a classical encryption algorithm. 3D Arnold cat map is shown as Eq.1.

$$\begin{bmatrix} F'x \\ F'y \\ F'z \end{bmatrix} = \left(\begin{bmatrix} 1 & a & b \\ c & ac+1 & bc \\ d & abcd & bd+1 \end{bmatrix} \begin{bmatrix} Fx \\ Fy \\ Fz \end{bmatrix} \right) \bmod (N) \quad \ldots. (1)$$

Where a, b, c, d and e are positive integers, F_x and F_y is the original pixel positions while F'_x and F'_y is scrambled pixel positions. F_z is a temp parameter and F'_z is scrambled pixel value.

2) Chaotic Map: The technology of image encryption that based on chaos is a code encryption technology that having developed in recent years. It looks upon the original image as the binary data stream that according to some encoded mode, then encrypts the image by using chaotic signal. The reason that Chaos is fit to image encryption is closely related dynamics characteristics. The chaotic signal has natural concealment, high sensibility to initial condition and to tiny perturbation motion, all those make the chaotic signal has an ability of long time unforeseeable. The security of this encryption system depends on the approximation between signal and random numbers that produced by secret key stream generator (be chaotic). The secret key stream is getting higher security as it approaching random numbers, whereas it is easily to be broken through.

3) Logistic Map: Logistic Map is an example among nonlinear equation which can be applied on the experiment mathematic studies triumphantly. Although it is simple, it can embody all the nature of nonlinearity phenomenon. Its function is shown as Eq. 2

$X_{n+1} = f(\mu, X_n) = \mu X_n (1-X_n)$ …. (2)

Where $\mu \in (3.57,4]$, $X_n \in (0,1)$. If $\mu = 4$ then the system is in chaotic state, and the sequence that the system produces now has the characteristics of randomness, erotic, and the sensibility to original value. And the range of it is (0,1). All these characteristics can provide a very good maintenance for the image encrypt operation.

C. Rubik's Cube

Erno Rubik, a Hungarian Physics professor invented the Rubik's cube technique in 1974, which has been utilized to change and scramble the position of the pixels of an image. In a classic Rubik's Cube, each of the six faces is covered by nine stickers, among six solid colours. Every face could be rotated clockwise or counter clockwise. Suppose one step indicates a 90 degree rotation, with three middle level of the cube, it has 18 different rotating methods for one step. It means we consider a step to be any quarter turn of a face, also known as the face-turn metric. We do not consider the alternative quarter-turn metric, which defines a half-turn to be two rotating steps. This principle provides permutation of the original image where two random keys are used to permute the rows and columns to provide the final permuted image. Shuffling of the pixels using the Rubik's cube technique results in a double ciphered image.

A normal 3 x 3 x 3 Rubik's Cube can have $(8! \times 3^{8-1}) \times (12! \times 12^{12-1})/2$ different positions, or about 4.3×10^{19}, forty-three quintillion (short scale) or forty-three trillion (long scale). The large number of permutations is given as a measure of the Rubik's Cube's complexity.

III. DESIGN APPROACH

The proposed encryption and decryption scheme has been divided into three stages, namely the LSIC, Arnold Transform and Rubik's Techniques. As a first step, the input DICOM image of size 256 x 256 was divided into 8-bit planes and was subsequently swapped to shuffle the same. By keeping this operation as seed, the tri-layer encryption scheme, namely LSIC, Arnold, Rubik's cube, was implemented. The decryption scheme was performed with the respective keys of all of the three stages to obtain the original image.

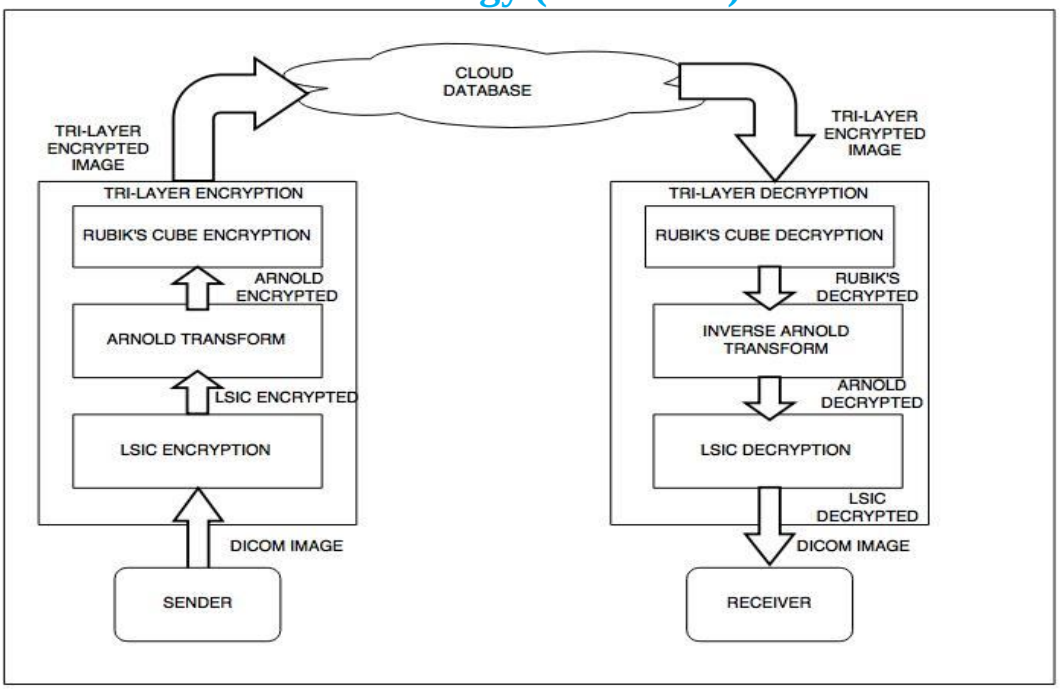


Figure. 1.2: System Architecture

IV. PROPOSED ALGORITHM

A. *Encryption*

1) *Latin Square Image Cipher:* A Latin square of order N is an N x N array filled with a set of N distinctive symbol elements, where each symbol appears exactly once in each row and each column. The name Latin Square is motivated by the mathematician Leonhard Euler, who used Latin characters as symbols. Mathematically, we define a Latin square L of the order N by an indicator function f_L on tri-tuple (r,c,i) as follows

$$f_L(r, c, i)=\begin{cases}1, & L(r,c) = S_i \\ 0, & otherwise\end{cases}$$

where r denotes the row index of an element in L with r □ N = {0,1,….., N-1}; c denotes the column index of an element in L with c □ N; i denotes the index of a symbol element in L with I □ N; and S_i is the i^{th} symbol in the symbol set S = {S_0, S_1, ….. S_{N-1}}.

2) *Algorithm :* A Latin Square Generator L=LSG(Q_1 ,Q_2)

Input: Q_1 and Q_2 are two length-N sequences
Output: L is a Latin square of order N
Q_{seed} =SortMap(Q_1)
Q_{shift}=SortMap(Q_2)
for r=0:1:N-1 do
L(r,:) = RowShift(Q_{seed},Q_{shift}(r))
end for

3) *Algorithm: Input:* K is a 256-bit key: P is a 256 x 256 8-bit grayscale image block

Output: C is a 256 x 256 8-bit grayscale image block
(Q_1 , Q_2)=KDSG(K,8)
for n=0 : 1 : 7 do
if n==0 then

C_{LSP} = LSBNE(p)[a]
end if
L_n=LSG(Q_1^n , Q_2^n)
D_n=L_n (0 , 0)
C_{LSW}=ECR_w(L_n, C_{LSP} , D_n)
if mod(n,2) ≠ 0 then
C_{LSS} =ECR_s^{col}(Ln , C_{LSW})
else
C_{LSS}=ECR_s^{row}(L_n , C_{LSW})
end if
C_{LSP} =ECR_p (L_n , C_{LSS})
L_8 = LSG (Q_1^8 , Q_2^8)
D_8 = L_8 (0 , 0)
C = ECR_W (L_8 , C_{LSP} , D_n)

4) Key Dependent Sequence Generator(q_1 , q_2)= KDSG(key, m)

Input: K is a 256-bit key; n is a nonnegative integer
Output: Q_1 = {Q_1^0,..,Q_1^M} and Q_2 = {Q_2^0,..,Q_2^M} are n-element set of random sequences, each of a length 256.

K_0 = K
for n = 0 : 1 : M do
[k_0 , k_1 ,…,k_7] = SKD (K_n)
for i = 0 : 1 : 8 do
$q^i(0)$ = PRNG(k_i)
for j = 1 : 1 : 63 do
$q^i(j)$ = PRNG(q^i(j - 1))
end for
end for
Q_1^n = [q^0 (0 : 31), q^1 (0 : 31), ……., q^7 (0:31)]
Q_2^n = [q^0 (32 : 63), q^1 (32 : 63), ……., q^7 (32:63)]
K_{n+1} = [q^0 (63), q^1 (63), ……., q^7 (63)]
end for

5) Image Encryption Algorithm based on 3D Arnold Cat

a) Initial value of logistic x0, product a sequence {x_0 , x_1 ,…..x_n}.
b) (2) Enlarge the sequence 1000 times, and then get the part of integer.
c) (3) Using mod (256) to get the final sequence {k_0, k_1, …k_n} (k □ [0,255]).
d) (4) Initial value of a, b, c, d, e and K to iterate K times to get position scrambled image.
e) (5) ϕ(X_i)={k_0, k_1,…,k_n}.
f) (6) Calculate F_z ⊕ ϕ (X_i) ⊕ A_i to get pixel value scrambled image.

Rubik's Cube

Modified Rubik's Cube Image Encryption Algorithm

(1) on pixels' shuffling procedure:

(a) rows and columns are alternatively shuffled (i.e., a row followed by a column, at a time),

(b) each row's and column's circular-shifting direction and number of steps is derived from their intrinsic properties, using different modulo operators;

(2) on pixels' ciphering procedure:

(a) maintaining the rule of alternating rows and columns, the shuffled image is doubly ciphered, using two different ciphering matrices,

(b) ciphering matrices are built using bit streams generated by chaotic systems, in conjunction with a multilevel

discretization method.

Algorithm

With I_0 representing the pixels values matrix of an 8-bit gray level scale image of the size m x m, the steps of newly proposed encryption algorithm are as follows.

(1) Randomly generate $\square_{max}$, no. of iterations, $\square_1$, $\square_2$, rows' & columns' modulo operators; initialize $\square$ to 0.

(2) For i=1:m,

(a) Compute the sum of all elements in row i

$S_{row\_i} = \sum_{j=1}^{m} I_0(i,j)$, ……. (1)

(b) Compute modulo $\square_1$ of S_{row_j}

$M_{row\_i} = S_{row\_j} (\text{mod } \square_1)$, ……. (2)

(c) Compute modulo 2 of M_{row_j}

$\square_{row\_i} = M_{row\_i} (\text{mod } 2)$, ……. (3)

(d) if $\square_{row\_i}$ = 0 -> row i is right circular-shifted, with M_{row_i} steps; else, if $\square_{row\_i}$ =1-> row i is left circular-shifted, with M_{row_i} steps

(e) Compute the sum of all elements in column i

$S_{col\_i} = \sum_{j=1}^{m} I_0(j,i)$, ……. (4)

(f) Compute modulo $\square_2$ of S_{col_j}

$M_{col\_i} = S_{col\_i} (\text{mod } \square_2)$, ……. (5)

(g) Compute modulo 2 of M_{row_j}

$\square_{col\_i} = M_{col\_i} (\text{mod } 2)$, ……. (6)

(h) if $\square_{col\_i}$ = 0 -> column i is up circular-shifted, with M_{col_i} steps; else, if $\square_{col\_i}$ =1-> column i is down circular shifted, with M_{col_i} steps.

(3) Increment a; if $\square \leq \square_{max}$, go to the previous step; else, go to the next step.

Steps (2)-(3) will modify matrix I_0 , generating a newly one denoted as I_{HVPS} (i.e., with horizontal and vertical pixels shuffled).

(4) Compute ciphering matrices I_{cipher_col} and I_{cipher_row}

(5) For i=1:m,

(a) cipher row i

$I_{HVPS}(i,:) = I_{HVPS}(i,:) \oplus I_{cipher\_row}(i,:)$, …….(7)

(b) cipher column I

$I_{HVPS}(:,i) = I_{HVPS}(:,i) \oplus I_{cipher\_col}(i,:)'$,……. (8)

Step(5) will modify the matrix I_{HVPS} , generating a newly one denoted as I_{ENC}.

B. Decryption

1) Rubik's Cube Decryption Algorithm: With I_{ENC} representing the pixels values matrix of an 8-bit gray level scale encrypted image of size m x m, with the correct key K=(□□□□□□□,x,r), the original image I_0 is recovered as follows.

a) Compute ciphering matrices I_{cipher_col} and I_{cipher_row}

b) For i=1:m,

i. decipher row i

$I_{ENC}(i,:) = I_{ENC}(i,:) \oplus I_{cipher\_row}(i,:)$, ……. (9)

ii. decipher column i

$I_{ENC}(:,i) = I_{ENC}(:,i) \oplus I_{cipher\_col}(i,:)'$, ……. (10)

Step(2) will modify the matrix I_{ENC} , generating a newly one denoted as I_{DEC} .

c) Initialize $\square$ to zero.

d) For i=1:m,

e) Compute the sum of all elements in column i

$S_{col\_i} = \sum_{j=1}^{m} I_{DEC}(j, (m+1-i))$, ……. (11)

(b) Compute modulo $\square_2$ of S_{col_j}

$M_{col\_i} = S_{col\_i} (\text{mod } \square_2)$, ……. (12)

(c) Compute modulo 2 of M_{col_j}

$\square_{col\_i} = M_{col\_i} (\text{mod } 2)$, ……. (13)

(d) if $\square_{col\_i} = 1$ -> column i is up circular shifted, with M_{col_i} steps; else, if $\square_{col\_i} = 0$-> column i is down circular shifted, with M_{col_i} steps,

(e) Compute the sum of all elements in row i

$S_{row\_i} = \sum_{j=1}^{m} I_{DEC}((m+1-i),j)$, ……. (14)

(f) Compute modulo $\square_1$ of S_{row_j}

$M_{row\_i} = S_{row\_j} (\text{mod } \square_1)$, ……. (15)

(g) Compute modulo 2 of M_{row_j}

$\square_{row\_i} = M_{row\_i} (\text{mod } 2)$, ……. (16)

(h) if $\square_{row\_i} = 1$-> row i is right circular shifted, with M_{row_i} steps; else, if $\square_{row\_i} = 0$-> row i is left circular shifted, with M_{row_i} steps.

(5) Increment $\square$; if $\square\square \leq \square\square_{max}$, go to the previous step; else, the decryption process is done.

Steps (4)-(5) will modify the matrix I_{DEC}, generating a new one denoted as I_0 (i.e., representing the pixel values matrix of the deshuffled image ~ the original image).

2) Inverse Arnold Transform Algorithm

a) Initial value of logistic x0, product a sequence $\{x_0, x_1, \ldots x_n\}$.
b) Enlarge the sequence 1000 times, and then get the part of integer.
c) Using mod (256) to get the final sequence $\{k_0, k_1, \ldots k_n\}$ ($k \square [0,255]$).
d) Calculate the period T of 3D Arnold Cat Map of NxN.
e) Initial value of a, b, c, d, e.
f) Iterate (T-K) times to get original image.
g) $\phi(X_i)=\{k_0, k_1, \ldots, k_n\}$.
h) Calculate $F_z \oplus \phi(X_i) \oplus A_i$ to get original pixel value image.

3) Latin Square Image Cipher Decryption Algorithm

Input : K is a 256-bit key: C is a 256 x 256 8-bit grayscale image block
Output: P is a 256 x 256 8-bit grayscale image block
(Q_1, Q_2)=KDSG(K,8)
for n=7: -1 : 0 do
if n==7 then
$L_8 = LSG(Q_1^8, Q_2^8)$
$D_8 = L_8 (0, 0)$
$P_{LSW}=DCR_w(L_8, C, D_8)$
end if
$L_n=LSG(Q_1^n, Q_2^n)$
$D_n=L_n (0, 0)$
$P_{LSP} = DCR_P(L_n, P_{LSW})$
if mod(n,2) $\neq$ 0 then
$P_{LSS} =DCR_s^{col}(Ln, P_{LSP})$
else
$P_{LSS}=DCR_s^{row}(L_n, P_{LSP})$
end if
$P_{LSW} =DCR_W (L_n, P_{LSS}, D_n)$ end for
P=P_{LSW}

V. IMAGE ANALYSIS AND METRICS

A. Correlation of Pixels

To analyse the performance of the proposed tri-layer cryptic effects, a correlation of the pixel values for the considered image for prior and post cryptic operations was computed. Horizontal (H), vertical (V) and diagonal (D) correlation values of the encrypted DICOM test images. Generally, the correlation value of one indicates high correlation, and zero points to obscurity among the pixels. The image encryption standard are necessitated to provide zero correlation values. Two adjacent pixels for vertical, horizontal and diagonal directions were selected, and the correlation coefficients (r_{xy}) were calculated, where x, y are the adjacent pixels in an image.

1) *Entropy Analysis:* Entropy determines the uncertainty in the final encrypted image. The value of this entropy should be close to 8 to prove the robustness of the algorithm.

2) *Differential Attacks:* Differential attacks were performed to analyse the strength and endurance level of the proposed algorithm. This technique was implemented by observing one pixel in the plain image and the corresponding change in the resultant image. If the change is evident in the resultant image, then it is asserted that the attack is rendered useless. There are two major constraints of differential attacks, namely NPCR and UACI. NPCR is the evaluation between two images by considering the corresponding pixel values with dissimilar grey levels. UACI is defined as the average intensity difference between the pixels in grey level for the two images.

VI. RESULTS AND DISCUSSION

Three stages of the encryption schemes have been performed. From the histograms of the final encrypted images, the pixel distribution was uniform, has a homogenous variation and is hence hard to crack by hackers.

Correlation distributions of adjacent pixels, one can observe that the adjacent pixels are highly correlated, and the correlation coefficient values are very high for the original images. The negative horizontal, vertical and diagonal values confirmed the smallest correlation between the original and encrypted images.

A. Key Space and Sensitivity Analysis

Key space represents the total number of distinct keys that can be used in encryption and decryption algorithms. A 256-bit key was used in the LSIC algorithm and a 5-bit key in the Rubik's encryption principle. The total key size for an 8-bit pixel is 256 x 5 x 8=10,240, and hence, the key space of the proposed system is 2^{10240}, which makes any brute force attack fail to determine the secret key. The key space of the proposed scheme is found better than the existing results.

Key sensitivity is primarily dependent on the algorithm used for encryption and decryption. The original image was encrypted by employing a secret encryption key, and the encrypted output. Following this, decryption was performed using the correct key, which resulted in a decrypted image. To verify the effectiveness of the implementation, the correct secret key was modified by changing only one character for the least significant character. This test revealed the key sensitivity of the proposed algorithm and the sensitivity is found to be better than the available schemes.

B. AWGN Channel attacks

AWGN is a basic channel noise model used in any information system considering randomness. In the proposed work, an encrypted image was transmitted over an AWGN channel noise model at various noise levels ranging from 0 to 25 dB. One can observe the sternness of test image against AWGN channel attacks, while test image was affected very severely. From the NPCR values, it has also been validated that one can decrypt the original image even after channel attacks.

C. Complexity Analysis

The proposed methodology involves three stages, LSIC, Arnold, Rubik's encryption schemes. LSIC involves two keys, key1 of size 10-bit and key2 of size 5-bit, and it involves nine iterations. Similarly, a 256-bit key and 8 iterations were used for Arnold. Finally, for Rubik's encryption, the input image will be taken as key1 and key2 and has 5 bits. So, the complexity of the proposed scheme is $2^{10}x2^{5}x9x2^{256}x8x2^{5}x8$.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

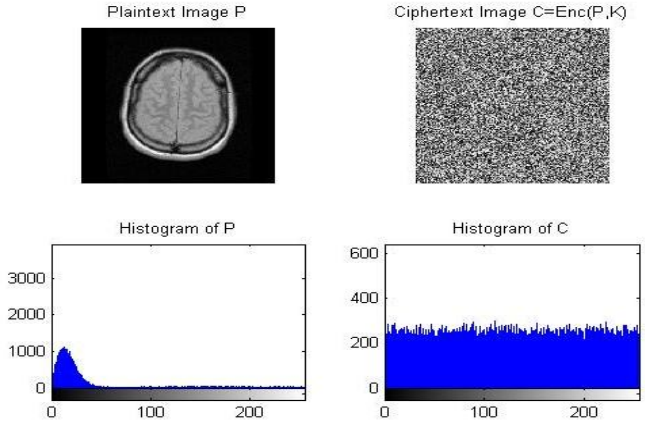


Figure 1.3: Latin Square Image Cipher Encryption

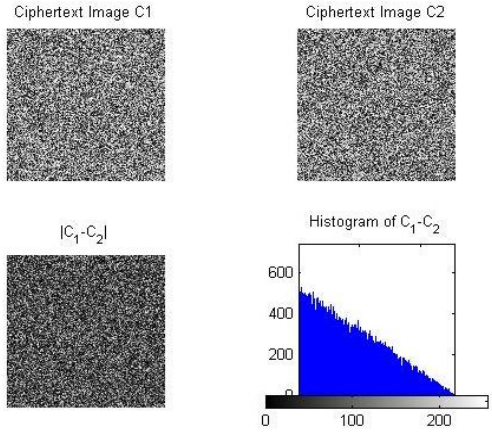


Figure 1.4: Probabilistic Encryption

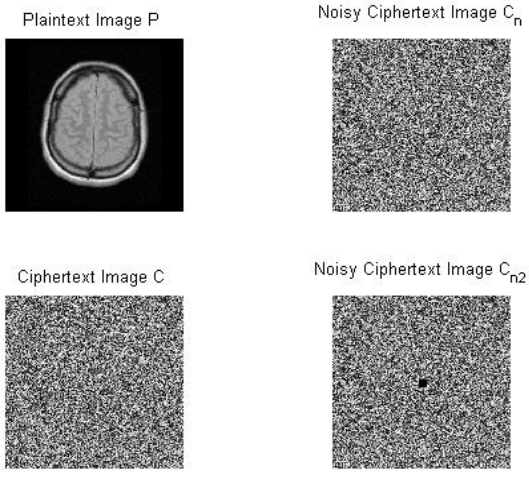


Figure 1.5: Robustness to Noise in Cipher Text

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

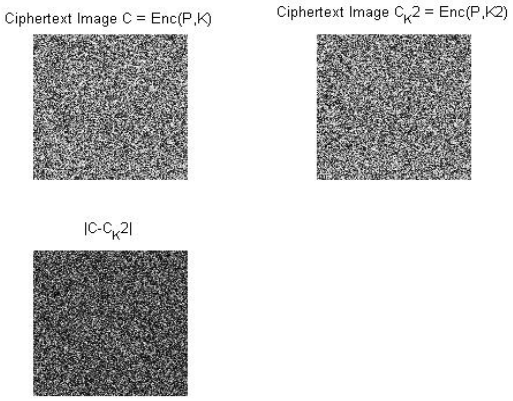


Figure 1.6: Sensitivity to Key Changes

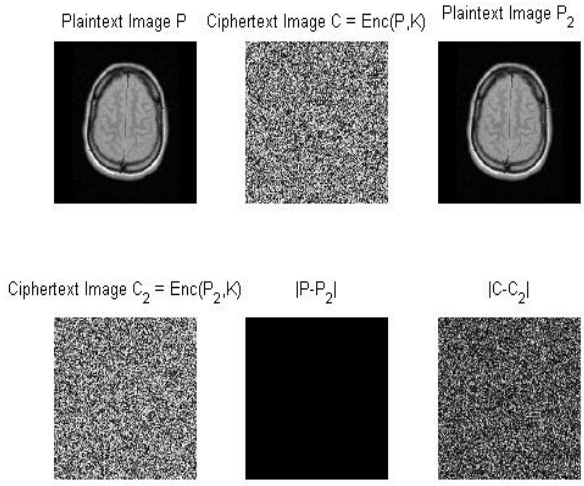


Figure 1.7: Sensitivity to Plain Text Changes

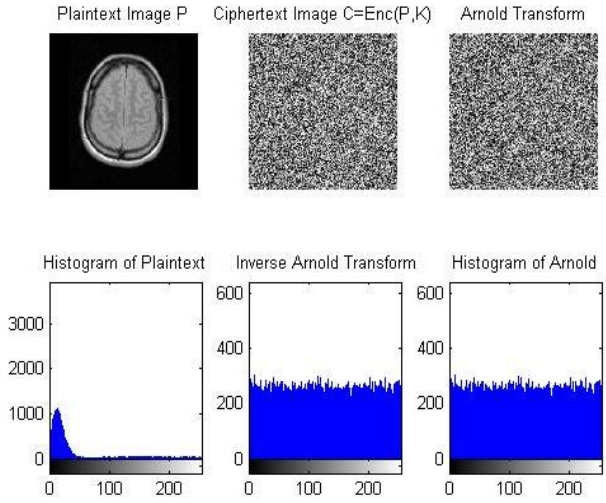


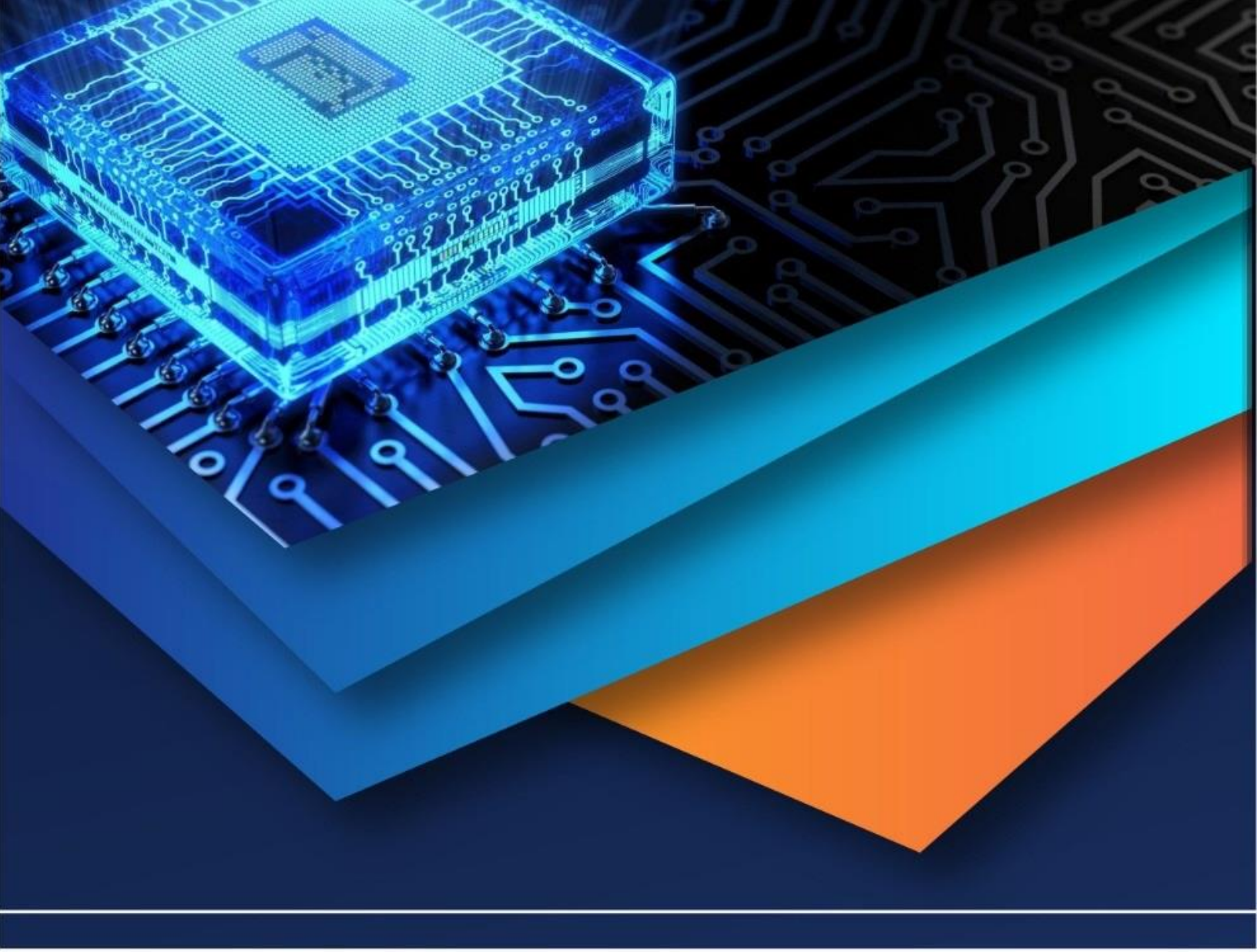
Figure 1.8: Arnold and Inverse Arnold Transformation

VII. CONCLUSION

A tri-layer image encryption technique was proposed and successfully implemented. LSIC, Arnold and Rubik's encryption operations on the host image yielded efficiently encrypted data, which resulted in better confusion, diffusion, permutation, tamper proofing and authentication. Then the technique was also tested by estimating the image quality metrics. The proposed methodology proved to be a secure and efficient algorithm for medical image transmission and reception. It can be applied to enhance security features by incorporating the quick response (QR) codes for the patient details in the encrypted images.

REFERENCES

[1] Kanso, A., Ghebleh, M,: A novel image encryption algorithm based on a 3D chaotic map. Commun. Nonlinear Sci. Numer. Simul. 17, 2943-2959(2012).
[2] Wang, X., Jin, C.: Image encryption using Game of Life permutation and PWLCM chaotic system. Opt. Commun. 285, 412-417(2012).
[3] Zhang, G., Liu, Q.: A novel image encryption method based on total shuffling scheme. Opt. Commun. 284, 2775-2780 (2011).
[4] Liu, Z., Gong, M., Dou, Y., Liu, F., Lin, S., Ashfaq Ahmad, M., Daia, J.,& Liu, S.: Double image encryption by using Arnold transform and discrete fractional angular transform. Opt. Lasers Eng. 50, 248-255 (2012).
[5] Pan, T., Li, D.: A Novel Image Encryption Using Arnold Cat. Int. J. Secur. Its Appl. 7, 377-386 (2013).
[6] Li, H.: Image encryption based on gyrator transform and two-step phase-shifting interferometry. Opt. Lasers Eng. 47, 45-50 (2009).
[7] Panduranga, H.T., Naveen Kumar S.K., and Kiran.: Image encryption based on permutation-substitution using chaotic map and Latin Square Image Cipher. The European Physical Journal Special Topics. 223, 1663-1677 (2014).
[8] Yue Wu, Yicong Zhou., Joseph, P N., Sos Agaian.: Design of image cipher using latin squares. Information sciences, 264, 317-319 (2014).
[9] Varsaki, E.E., Fotopoulos, V., Skodras, A.N.: A discrete Gould transform data hiding scheme. Math. Meth. Appl. Sci. 37, 283-288 (2014).
[10] Adrian-Viorel Diaconu., Khaled Loukhaoukha,: An Improved Secure Image Encryption Algorithm Based on Rubik's Cube Principle and Digital Chaotic Cipher. Mathematical Problems in Engineering 2013, 1-10 (2013).
[11] Li Zhang., Xiaolin Tian., Shaowei Xia.: A Scrambling Algorithm of Image Encryption Based on Rubik's Cube Rotation and Logistic Sequence. International Conference on Multimedia and Signal Processing (CMSP), 312-315 (2011).
[12] Shun Zhang., Tiegang Gao., and Lin Gao.: A Novel Encryption Frame for Medical Image with Watermark Based on Hyperchaotic System. Mathematical Problems in Engineering, 240749, 1-11 (2014).
[13] Kannammal, A., Subha Rani, S.: Two level security for medical images using watermarking/encryption algorithms. International Journal of Imaging Systems and Technology, 24, 111-120 (2014).
[14] Muhaya, F.B., Usama M., Akhter, F.: Chaos based secure storage and transmission of digital medical images. Applied Mathematics and Information Sciences, 8, 27-33 (2014).
[15] Al-Haj, A.: Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. Journal of Digital Imaging, 9 p. Article in Press (2014).
[16] Kiah, M.L.M., Ahmed Haiqi, Zaidan, B.B., Zaidan, A.A.: Open source EMR software: Profiling, insights and hands-on analysis. Computer Methods and Programs in Biomedicine, 117, 360-382 (2014).
[17] Zhang, Y., Xiao, D., Liu, H., Nan, H.: GLS coding based security solution to JPEG with the structure of aggregated compression and encryption. Commun. Nonlinear Sci. Numer. Simul. 19, 1366-1374 (2014).
[18] Zhang, X., Qian, Z., Feng, G., Ren, Y.: Efficient reversible data hiding in encrypted images. J. Vis. Commun. Image Represen. 25, 322-328. (2014).
[19] Lee, M.H., Khan, M.H.A., Kim, K.J., Park, D.: A fast hybrid Jacket-Hadamard matrix based diagonal block-wise transform. Signal Process. Image Commun. 29, 49-65 (2014).
[20] Armand Eyebe Fouda, J.S., Yves Effa, J., Sabat, S.L., Ali, M.: A fast chaotic block cipher for image encryption. Commun. Nonlinear Sci. Numer. Simul. 19, 578-588 (2014).
[21] Wu, X., Bai, C., Kan, H.: A new color image cryptosystem via hyperchaos synchronization. Commun. Nonlinear Sci. Numer. Simul. 19, 1884-1897 (2014).
[22] Gonzalo Alvarez, Shujun Li., Luis Hernandez.: Analysis of security problems in a medical image encryption system. Computers in Biology and Medicine, 37, 424-427 (2007).
[23] Chong Fu, Wei-hong Meng, Yong-feng Zhan, Zhi-liang Zhu, Francis C.M., Lau, Chi K. Tse, Hong-feng Ma.: An efficient and secure medical image protection scheme based on chaotic maps. Computers in Biology and Medicine, 43, 1000-1010 (2013).
[24] Dang, P.P., Chau, P.M.: Image encryption for secure Internet multimedia applications. IEEE Trans. Consum. Electron. 46, 395-403 (2000).
[25] Padmapriya Praveenkumar, Rengarajan Amirtharajan, K. Thenmozhi, John Bosco Balaguru Rayappan.: Medical data sheet in safe Havens – A tri-layer cryptic solution, Computers in Biology and Medicine. (2015).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY