**Bulletin of Electrical Engineering and Informatics**
**ISSN: 2302-9285**
Vol. 5, No. 3, September 2016, pp. 347~365, DOI: 10.11591/eei.v5i3.544 

# A Naïve Visual Cryptographic Algorithm for the Transfer of Compressed Medical Images

**Shivaputra*[1], H. S. Sheshadri[2], V. Lokesha[3]**
[1]Department of ECE, Dr. Ambedkar Institute of Technology, Bengaluru, India
Research Scholar, Jain University, Bengaluru, India
[2]Department of ECE, PES College of Engineering, Mandya, India
[3]Department of Mathematics, Vijayanagara Sri Krishnadevaraya University, Bellary, India
*Corresponding author, e-mail: shivaputra@dr-ait.org

***Abstract***

*The transmission of a suitably compressed image over a bandwidth, over long distances, gives rise towards a new era in the field of information technology. A gradual increase in this appending scenic application, involving the transfer of the images securely over the Ethernet has become an increasingly important aspect to be addressed during thou phenomenon, especially in the transfer of the digital medical images vividly, encapsulated with abundant information related to these images. The compressed medical images of the DICOM format contain certain amount of confidential data, pertaining to a clinical research or to an individual, and the confidentiality of the same has to be preserved from various security threats and eves-dropping. With a widespread applications among various multimedia applicative systems, telemedicine, medical imaging, military and certain safety-critical applications, inter-net and intra-net communicative applications, etc, a reliable transfer of suitable information, efficiently & securely is considered as one of the revolutionary aims in today's communication technology and visual cryptographic methodologies. Real-time applications as such detailed above majorly is concerned with the security measures and many algorithms have been developed as a proof for various visual cryptographic methodologies. In this paper we propose an efficient and a reliable visual cryptographic methodology which focuses on the encryption and decryption of the two-dimensional DICOM standard compressed medical image, effectively. This paper discusses an efficient design of 192 bit encoder using AES Rijndael Algorithm with the decomposition of an image into square image size blocks and the image blocks are shuffled using 2D CAT map. The shuffling of the image blocks/pixels employs a Logistic map of these image pixels coupled with 2D mapping of the pixels of the DICOM standard medical image, generated randomly, being the control parameter thereby creating a confusion between the cipher and the plain image, gradually increasing the resistive factor against the significant attacks. This paper proposes various analytical metrics such as correlation analysis, entropy analysis, homogeneity analysis, energy analysis, contrast and mean of absolute deviation analysis, to evaluate the proposed algorithm, and their suitability in image encryption applications.*

***Keywords****: Chaotic Maps, Image Shuffling, Logistic Map, Image Encryption & Decryption, Correlation Co-efficient, Homogeneity, Key Space Analysis*

## 1. Introduction

Among the wide range of applications that claim to be multimedia, with diverse target areas as E-magazines, Video-On-Demand (VOD), distance learning, WAN virtual reality, telemedicine, health monitoring systems, etc., these applications are sorted into categories such as

a. *Information Systems*: An exhaustive multimedia application category wherein the main purpose of all the systems in this category is the provision of the information to the user. This category again subcategorizes application areas as
   1) Electronic Publishing: E-papers, Electronic Newspapers.
   2) Hospital information Systems: Telemedicine, Health Monitoring Systems, Virtual Reality Surgery, Patients Databases - Multimedia form.
   3) Navigation & information Systems: Public spaces offering the interactive medium about the orientation of the outlets and other services available.
   4) Historic Locations & Museums: Online catalogs, Interactive Tours.
b. *Remote Systems*: The application involving multimedia wherein the systems are

*Received September 14, 2015; Revised June 4, 2016; Accepted June 18, 2016*

represented such that the users are at a remote location and the services are provided to such users. These systems are hard categorized into two categories as *passive* & *active systems.* A passive system representation includes users who either simply send or receive the information about a remote location and thou actions takes place at that particular location of the user. On the other hand the active representation notably involves systems wherein the users take part in the process of action and as well influence the process at the remote location. Some of the applications involved in such representation of the systems are;

1) Conferencing: User along with other participants takes part in the conference from different remote locations. Sharing of different multimedia file types like text, graphics can be shared.
2) Distance Learning: Similar to sharing of different multimedia conference session, lectures or class materials is shared among different users.
3) Virtual Reality: Users in a physically-nonexistent environment can be made available through this application.
4) Remote Robotic Agents: Hazardous environments which may require human intervention may be carried out without their physical presence and by the deployment of robots in such environments.

c. *Entertainment Systems*: Lot of companies in the diverse field of telecommunication and media communications, are well suited with deployment and the employment of multimedia techniques.
   1) Digital Television: An advanced broadcasting technology which overcomes the typical analog broadcasting involving digital media with substantially higher quality and size (for example, *High Definition Television (HDTV)*).
   2) Interactive Television: The ability involving the users partake in the interactive sessions like voting, game shows etc, with the necessary technological infrastructure deployed at the station (for example, *Set-Top Boxes*)
   3) Video-On-Demand (VOD): Transmission of customized multimedia over the bandwidth.

With such a varsity of applications, the multimedia applications are as well prone to many security threats reigning from various impacts and their depending magnitudes.

## 2. Visual Cryptography and Image Encryption

Visual cryptography is a methodology or a technique which involves various multimedia such as audio, video, images, text, etc., being encrypted (converted to another suitable format), to maintain the authenticity of the multimedia content during its transmission over a suitable bandwidth. The main aim of these cryptographic techniques is to avoid eves-dropping and to decrease the probability of an attacker detecting the cryptosystem. This technique is highly recommended when there is a need for the transmission of the data between members of a certain group who can be entrusted with the security of the details of the multimedia. During the Visual Cryptography the set of users have to precisely be classified as *qualified* or *forbidden*. There are several factors/properties governing the deployment of Visual cryptography for insecure groups; and the highlights of them being

a. *Contrast*: For the recovery of an hidden message or information from a multimedia the qualified users can stack their transparencies and dependencies
b. *Security*: Restricting the users from deciding the conceptuality and the contents of the hidden image pixels, even with all their shares

The concept of cryptography in multimedia application, confirms the security content in communication, involving the process of encryption which places an important role in encoding the messages or the information contained in a suitable multimedia content, in a way wherein only the authenticated users are liable to access the information thou contained. The concept of encryption alone does not guarantee the interception of un-authorized users from accessing the content, but it prevents the forbidden users with the message content. Image encryption is one of the applications of the visual cryptographic methodologies involved in the encryption of the suitable image. The cryptographic techniques used for the multimedia applications are closely related to various other techniques such as *encryption, multimedia compression & communication, etc.* The process of encryption entitles with the encrypting of the multimedia content based on the traditional encryption methodologies. The multimedia content compression

is to be inclusive of the compression techniques before, during or after. But since a compressed multimedia content before the transmission procedure or storage saves cost and bandwidth metrics, a before transmission compression is considered here in the proposed work. The vibrant multimedia communication techniques require such efficient encryption and decryption methodologies in converging the data privacy.

## 3. Survey for the Literature

The ever increasing growth of multimedia applications requires a high role in terms of the security issues while its use in the communication over a bandwidth and storage of such files for further applicative uses. Visual Cryptographic methods like the encryption of the image/video was evolved to address the above issues, wherein an image or a video is converted into another image, which will be unable to understand by the third party between a communication between two users, and requires a key to understand or decrypt the encoded image in the retrieval of the original image. In 2007, M. Zeghid et.al [4] proposed an efficient encryption standard in order to encode an image, the Advanced Encryption Standard (AES), and in this technique a key generator such as a key stream generator was included. This ensured the improvement of the proposed AES encryption performance. The original image was divided into blocks; all these blocks were rearranged to produce a transformed image by means of a transformation algorithm. Thou transformed image was encrypted using the Blowfish algorithm. This image encryption methodology using block-based transformation algorithm was proposed by Mohammad Ali Bani Younes et.al (2008) [5]. The proposed work provided substantial proofs to show a decrease in the correlation between the image elements. They also provided justifiable results with a lower correlation and higher entropy values. In 2008, Saroj Kumar Panigrahy et.al [6] presented an image encryption technology by making use of the Hill ciphers. A self-invertible key matrix was generated by the Hill cipher algorithm, which was used to encrypt both the gray-scale as well as the colour images. This algorithm was efficient for images with a different gray level or colour background. This was one of the drawbacks with this algorithm wherein the inefficiency was highlighted with an image with the same gray level or the same colour background. Later in 2008 Aman Jantan et.al [7] introduced a new technique based on the combination of the image permutation and an encryption algorithm by Rijndael, as Rijndael algorithm. In this methodology the image was divided into a 4X4 pixel block and was rearranged using a process of permutation to form a permuted image and later encrypted using the Rijndael algorithm. Bibhudendra Acharya et.al (2009) [8] proposed an advanced Hill cipher algorithm (AdvHill). This algorithm uses an involutory key matrix for encryption. Of lately in 2009 Zhang Yun-Peng et.al [9] proposed a Digital image encryption algorithm based on chaos and improved DES algorithm. They used the logistic chaos sequencer in generating the pseudo-random sequence which also carries the RGB information of the image to the image chaotically and thus the image is encrypted with the improved DES algorithm. Later in 2010, Seyed Mohammad Seyedzade et.al [10] came up with a novel image encryption algorithm based on the Hash function, based on SHA-512 hash function. This particular approach can be divided into subsections wherein firstly a pre-processing of the image is done by shuffling the image pixels in one half of the image. Secondly the considered has function is used to generate a mask of a random number and this mask is XORed with the other part of the image, to be encrypted. A Digital Image encryption algorithm was proposed by Ismail et.al in 2010 [11]. This algorithm was based on composition of two Chaotic Logistic maps which introduces an efficient chaos-based stream cipher, and has two chaotic logistic maps with a large external secret key for the process of image encryption.

Kamali S.H et.al [12], proposed a new modified version of Advanced Encryption Standard (MAES) to reflect a high level of security and a better image encryption algorithm. The resultant of this algorithmic implementation was high image security. In 2011, Rasul Enayatifar et.al [13] proposed a new method, which was based on genetic algorithm with the evolution of a hybrid model and a chaotic function for the encryption of the image. Later Tariq Shah Et.al [14] in 2011, came up with a statistical analysis of S-box in image encryption applications based on the majority logic criteria monitoring the process of encrypting the image. Their study being the back bone for the evolution of the work proposed in this paper. Their analysis yielded the particulars and the characteristics of the prevailing S-boxes and their strengths and

weaknesses, providing a strong support in the development of an efficient image encryption algorithm.

## 4. Proposed Methodology

The methodology adopted in this work and explained in this literature considers the image encryption methodology. The process involved here includes the consideration of the compressed DICOM standard medical image, using the hybrid lossless image compression techniques for ROI and Non-ROI regions [2]. Thou compressed image is input into this encryption algorithm machine for encrypting the image data for transmission and storage. The algorithm machine considered in this literature involves 2 major blocks & 1 process;

a. CAT Mapping–for image data block & pixel shuffling
b. AES Encryption Machine–for encrypting the plain compressed image or the information contained in the image.
c. Logistic Mapping Process–pre-process the image pixel blocks before it is input into the CAT Mapping machine for shuffling the image pixel blocks.

The first cycle of the engine starts with the initialization of the variables for the logistic mapping of the pixel blocks initially. The image pixel in-terms of x & y sequences are mapped for the image and is subjected to a pre-processing procedure to process all the pixel sequences in order to obtain the new ordered pixel blocks. The new values are mapped onto the terms $a_i$ & $b_i$, which are then input into the CAT Mapping machine. In the CAT Map machine, the pixels of the pre-processed image are first shuffled within the block set of the pixels of the image. Then the entire block-set is shuffled. In the next procedural step the pixels within the entire image block is shuffled in order to obtain a shuffled image. The resultant shuffled image is input with the image data/information to the AES Encryption block with the image representation or the image data representation in the form of 192 bits.

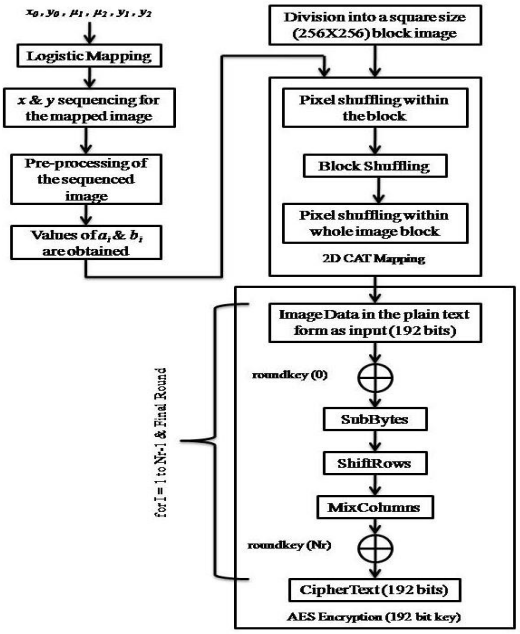


Figure 1. Proposed Methodology Workflow

The AES Encryption & Decryption is a symmetric cryptographic methodology, wherein the data length can be of 128, 192, 256 bit as well the key bit length for confiding the data can be of length 128, 192 or 256 bits. The image data is XORed with the round key to transform with the SubByte data. Then the resultant matrix array is shifted circularly and is transformed with the column mixing operations. The transformed matrix array is again XORed with the round key

for the final with the Nr words and thus we obtain the cipher text or the encrypted image. The process is iterative and is optimal as with the analysis of the metrics of image encryption. The related analytical values thus obtained prove out to be efficient with this algorithmic approach.

The steps involved in this proposed methodology are as follows;

a. The initial values of $x_0$, $y_0$, $\mu_1$, $\mu_2$, $y_1$, $y_2$ as per the Logistic Mapping expressions coupled over 2 Dimensions for the Logistic Coupling required for shuffling the image pixels.
b. *x* & *y* mean values are obtained from the sequences of the logistic mapped image values.
c. Pre-processing which involves stretching, folding, substitution of the image pixels are done and are mapped onto the new image pixel values as $a_i$ & $b_i$.
d. With the mean values of the image obtained, the image is input into the CAT Mapping algorithm in order to shuffle the image pixels within the blocks of the image.
e. Later the blocks of the image pixels are shuffled and thus we obtain a shuffled image as shown in Figure 2.

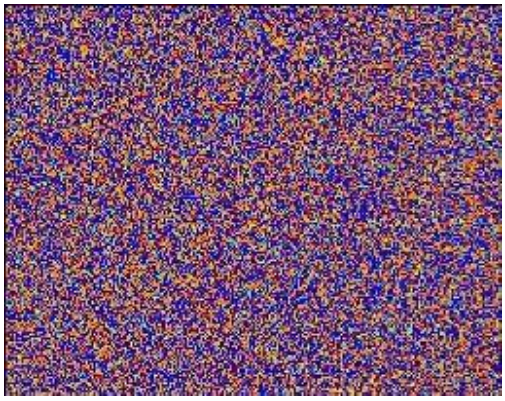

Figure 2. Shuffled Image after 2D CAT Map

a. The image data is then tapped from the shuffled image and is fed into the AES Encryption machine wherein the data undergoes the procedure of transformations such as SubByte, Mix Column, ShiftRow & AddRoundKey for the considered word length of 192 bits and key-length of 192 bits.
b. The modification is done with the S-Box obtained as

$$\begin{pmatrix} 63\ 7c\ 77\ 7b\ f2\ 6b\ 6f\ c5\ 30\ 01\ 67\ 2b\ fe\ d7\ ab\ 76 \\ ca\ 82\ c9\ 7d\ fa\ 59\ 47\ f0\ ad\ d4\ a2\ af\ 9c\ a4\ 72\ c0 \\ b7\ fd\ 93\ 26\ 36\ 3f\ f7\ cc\ 34\ a5\ e5\ f1\ 71\ d8\ 31\ 15 \\ 04\ c7\ 23\ c3\ 18\ 96\ 05\ 9a\ 07\ 12\ 80\ e2\ eb\ 27\ b2\ 75 \\ 09\ 83\ 2c\ 1a\ 1b\ 6e\ 5a\ a0\ 52\ 3b\ d6\ b3\ 29\ e3\ 2f\ 84 \\ 53\ d1\ 00\ ed\ 20\ fc\ b1\ 5b\ 6a\ cb\ be\ 39\ 4a\ 4c\ 58\ cf \\ d0\ ef\ aa\ fb\ 43\ 4d\ 33\ 85\ 45\ f9\ 02\ 7f\ 50\ 3c\ 9f\ a8 \\ 51\ a3\ 40\ 8f\ 92\ 9d\ 38\ f5\ bc\ b6\ da\ 21\ 10\ ff\ f3\ d2 \\ cd\ 0c\ 13\ ec\ 5f\ 97\ 44\ 17\ c4\ a7\ 7e\ 3d\ 64\ 5d\ 19\ 73 \\ 60\ 81\ 4f\ dc\ 22\ 2a\ 90\ 88\ 46\ ee\ b8\ 14\ de\ 5e\ 0b\ db \\ e0\ 32\ 3a\ 0a\ 49\ 06\ 24\ 5c\ c2\ d3\ ac\ 62\ 91\ 95\ e4\ 79 \\ e7\ c8\ 37\ 6d\ 8d\ d5\ 4e\ a9\ 6c\ 56\ f4\ ea\ 65\ 7a\ ae\ 08 \\ ba\ 78\ 25\ 2e\ 1c\ a6\ b4\ c6\ e8\ dd\ 74\ 1f\ 4b\ bd\ 8b\ 8a \\ 70\ 3e\ b5\ 66\ 48\ 03\ f6\ 0e\ 61\ 35\ 57\ b9\ 86\ c1\ 1d\ 9e \\ e1\ f8\ 98\ 11\ 69\ d9\ 8e\ 94\ 9b\ 1e\ 87\ e9\ ce\ 55\ 28\ df \\ 8c\ a1\ 89\ 0d\ bf\ e6\ 42\ 68\ 41\ 99\ 2d\ 0f\ b0\ 54\ bb\ 16 \end{pmatrix}$$

c. Encrypted Image data or the image is obtained.

## 5. Chaotic Mappings

Highly sensitive signals to the system initial conditions and parameters, also considered as the best for the practical use are the Chaos signals. They also are supposed to possess the pseudo-random properties and are non-periodical. Such signals which are chaos in nature are well suited for an efficient and a robust crypto-system like the system proposed in this work. Traditional encryption scenarios are difficult since the multimedia content like medical images as considered in this paper bears some inherent features like bulk data/information capacity and high data redundancy. Transmission of the images in real-time bandwidths over variant and vibrant communication channels have resulted in the evolution of many efficient ways and development of some specific standards for chaos based image encryption. One of the evolutionary products like 2D CAT mapping is used in our work. Many image encryption algorithms are proposed based on such chaotic systems and many improvement features involving the features like shuffling of the pixels or the blocks of pixels in an image, using the efficient chaotic maps are implemented along with some of the efficient encryption algorithms like Rijndael AES algorithm.

### 5.1. Logistic Mapping: 2D-coupled

The equations that describe the Logistic Mapping coupled over 2-dimensions are as follows;

$$x_{n+1} = \mu_1 x_n(1 - x_n) + \gamma_1 y_n^2$$

$$y_{n+1} = \mu_2 y_n(1 - y_n) + \gamma_2(x_n^2 + x_n y_n)$$

The strength of the above mentioned complexity of the Logistic map is enhanced by coupling the main three quadratic terms. The decision of the system being chaotic at suitable intervals of metric magnitudes, which are also estimated as follows;

$$2.75 < \mu_1 \leq 3.4$$

$$2.7 < \mu_2 \leq 3.45$$

$$0.15 < \gamma_1 \leq 0.21$$

$$0.13 < \gamma_2 \leq 0.15$$

The above magnitudes validates the system in the generation of the chaotic sequences *x* & *y* within the time-stamp of (0,1). The initial conditions and parameters considered in this work, runs for *n*=18200 times and the parameters being;

$x_0 = 0.0325$
$y_0 = 0.6843$
$z_0 = 0.4227$
$\mu_1 = 3.15$
$\mu_2 = 3.98$
$\gamma_1 = 0.210$
$\gamma_2 = 0.171$
$\lambda = 4.1679$

An analysis of these magnitudes for *x* and *y*, statistically exhibited a fair decrement in the relationship between the sequences, also with their correlative properties. The mean values of the sequences were computed as;

*mean(x)=0.7865*
*mean(y)=0.9759*

A pre-processing has to be performed to improve the statistical properties of the sequences *x* and *y,* generated by the logistic mapping coupled with 2D properties. The equations that monitor the pre-processing attributes are given as;

$$x_i = 10^6 x_i \; - \; floor(10^6 x_i)$$

$$y_i = 10^6 y_i \; - \; floor(10^6 y_i)$$

The pre-processed image is obtained before the image pixel blocks are shuffled and presented into the algorithm for shuffling, is as shown in Figure 3.

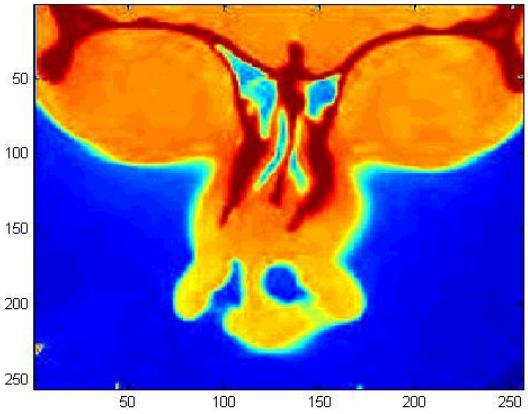


Figure 3. Pre-processed Image

This function appears to balance the correlation inheritance between the sequences *x* and *y.* Their respective mean values projects to be close to a relative value of 0.6, to be utilized for the cryptographic process and subject to be with the magnitudes as;

*mean(x)=0.5739 & mean(y)=0.5977*

### 5.2. CAT Mapping: 2D

Stretching and folding the trajectories of a 2D image, in a simple discrete system, proposed by Vladimir I Arnold in his work of research for the ergodic theory, of dynamic systems with measures in varying and their related problems. This theory accepts a 2D square image with certain properties, being the matrix of the image given as,

$$\Gamma \left( \begin{bmatrix} x \\ y \end{bmatrix} \right) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \; mod 1$$

wherein the image for the mapping Γ is considered to be *invertible,* having a matrix *determinant* 1 and the inverse of thou matrix having the entries with the type *integer.* The uniqueness of Γ has to be *hyperbolic fixed point,* with the vertices of the image being square.

A mapped image using the CAT map can be restored back to as the original image, with the number of iterations for the restoration not exceeding the factor 3N, where N is set to be an integer value. This restricts the position and the momentum variables to data types of integers and the mapping being toroidial with the square grid points within the image. The same concept of 2D CAT map has been successfully implemented and proposed in our work. The relationship between the *n* iterations is given as;

*n=0 :* $T^0(x, y) = Input\ DICOM\ Standard\ medical\ Image\ (x, y)$

*n=1:* $T^1(x, y) = T^0\left(mod(2x + y, N), mod(x + y, N)\right)$

$$\vdots$$

*n=k:* $$T^{k}(x,y) = T^{k-1}\big(mod(2x+y,N), mod(x+y,N)\big)$$

$$\vdots$$

*n=m:* $$Output\ Image(x,y) = T^{m}(x,y)$$

In the proposed work, the positions of the pixels of the compressed medical image are considered as I={(*x,y*) | *x, y*=1,2,3,.....,N}. The control parameters [15] for the mapping are monitored using the mathematical metrics as;

$$x' = (x + ay) mod(N)$$
$$y' = (bx + (ab + 1)y) mod(N)$$

The controlling parameters *a* and *b* are considered to be positive integers within the super-set of N, which a set of integers. The new position of the image pixels *(x',y')* is given by the equations mentioned above, from the original pixel position from the original plain image of N x N, given as *(x,y),* are obtained on processing the original DICOM medical image using the 2D CAT Mapping. The original positions of the pixels in the original plain image are reshuffled/permutated to the new co-ordinates monitored by the algorithm for 2D CAT Mapping. Since this mapping procedure is periodic in nature it appears as if the original image is obtained after suitable number of iterations. The image with the new co-ordinates or the reshuffled pixels, correlated with the adjacent pixels, distributed on the entirety of the image, while the image appears to be with distortions and meaningless. The control parameters are to be considered in the performance of the CAT Mapping in order to monitor the periodicity legacy [16] of iterating the original image, which are generated randomly for each 8 X 8 block within a 256 x 256 block image. The image obtained after the 2D CAT Map is as shown in

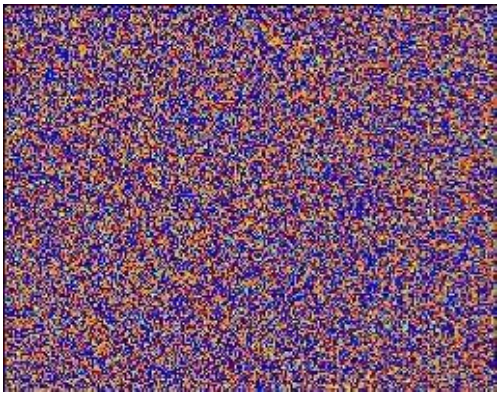

Figure 4. 2D CAT mapped shuffled image

## 6. AES Algorithm

Evaluation of different encryption algorithms on the basis of throughput, area of requirements and the execution speed accelerated the necessity for a secure mode for the exchange of large quantities of digital data. The need was addressed with classified cryptographic algorithms; symmetrically or asymmetrically. The Symmetric algorithmic systems included algorithms such as;

- *Data Encryption Standard (DES)*
- *3DES*
- *Advanced Encryption Standard (AES)*

The classification being made on the basis of the key between the accredited users, i.e. both the sender and the receiver. A case wherein both the sender and the receiver use an identical key to encrypt and decrypt the message contained in a multimedia content or a text is being categorized as Symmetric System.

- *Rivest-Shamir-Adelman (RSA)*

- *Elliptic Curve Cryptosystem (ECC)*

The above systems are categorized as Asymmetric Systems, wherein the systems uses different sets of keys for encrypting the message text/a message contained in a multimedia content and decrypting the encoded/cipher test/a message within a multimedia content . Since the applications involving the multimedia content posses in them large quantities of data Symmetric Systems are more widely accepted and recommended. This type of applications obligates for their functionalities, algorithms and systems which serves high speed transfers and crypt analyses. National institute of Standards and Technology (NIST) proposed the Advanced Encryption Standards (AES) as a replacement to Data Encryption Standards (DES). Joan Daemen at University of Leuven developed an efficient Rijndael algorithm which was later pronounced to one of the suitable algorithms with characterized metrics such as *security, performance, flexibility and adaptability* in terms of operations. This algorithm is also considered as one of the efficient schemes suitable for the encryption, dealing with both hardware and software aspects. The criteria being the improvisations in physical security at high data speeds, this was entitled as more suitable for hardware implementation of cryptographic systems, off-lately. Such kind of applications is dealt in military communications, medical transmissions, mobile telephony, etc. A Symmetric-key cipher, Advanced Encryption Standards (AES), is an encryption standard wherein the sender and the receiver use a single, unified key for the process of encrypting and decrypting the message content. The same has been used in this work. A standard medical, DICOM format image,

Figure ***5*** is considered which is supposed to contain huge quantity of data.

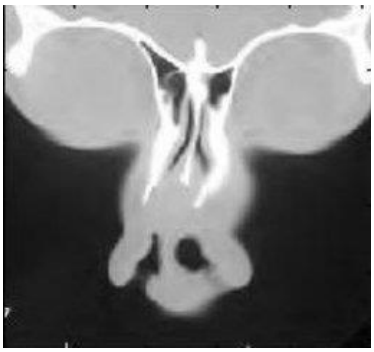

Figure 5. DICOM format compressed medical image

The length of the data blocks can be 128, 192, or 256 bits. Here in our proposed work we have considered a data block length of 192 bits. This standard algorithm is an iterative process, and each iteration is called as a *round.* The total number of *rounds* required depends on the length of the key considered. The key used in AES algorithm can be of lengths 128, 192 or 256 bits. If the key length considered is 128 bits then the number of rounds would be 10, while its 192 bits then the number of rounds would be 12, and 14 if the key length is 256 bits. The data block is respectively divided into bytes. SO in this work, since the length of the data block is 192 bits, it is divided into 24 bytes. These bytes are then mapped onto a standard array such as 4X4, called as the States. The operations such as *Shifting of the rows, Sub Bytes, mixing the Columns* are all performed on these States.

The parameters used in this paper, are in accordance with the key length as *Nk words,* given as 6. The block size as *Nb words* is 4 and the number of rounds given by *Nr* is 12.

### 6.1 Methodology Involved in the Design of 192 bit Encoder

The number of iterations in the AES algorithm is known as *rounds*. Since the AES algorithm involves an encryption process which is iterative by behavior. This process requires 192 bit key as for each round in the work proposed in this paper takes into consideration 192 bit input data block. As per the considerations of the AES parameters our algorithm requires 6 words in every one round for the process. The number of rounds decides upon the required number of words as 6, to which the input key has to be expanded. There appears to be

simplicity in the design of this algorithm, as this symmetric algorithm uses the same key both for encryption and decryption.

There happens to be transformations when the algorithm enters into each round of during the encryption process, of the algorithm. These transformations occur at various abstract levels during the metamorphosis of the plain text into a cipher text. The transformational procedures are;

a. *SubBytes:* In this transformational procedure each byte is operated individually and the transformed byte is substituted subsequently in the S-box.
b. *ShiftRow:* The rows of the State are technically shifted cyclically, across a range of offsets.
c. *MixColumn:* A suitable fixed polynomial is considered and is multiplied to the contents of the Column in the State, against the considered set of polynomials of the State, as GF ($2^8$).
d. *AddRoundKey:* The elements in the key matrix/block are XORed bit-wise.

A single data block of 192 bits, considered to be as a plain text from the medical standard compressed DICOM image, as in the work proposed in this paper is considered. The medical image of interest is suitably compressed using the Hybrid Compression algorithm [2] and later shuffled using the 2D CAT Map as explained in the above procedures. The State array, is a square matrix to which the 192 bits of the data block from the compressed and shuffled DICOM standard medical image, is transcribed. As when there is an update in the data block set, with the iterative rounds for shuffling and compression the same are modified at suitable times in the State array. The key block of 192 bits is also represented as bytes of square matrix. The bytes of key and the data block are sequenced by means of column in a matrix.

A linear array of 60 words (240 bytes) is produced by taking an input of 6-word (28 bytes) key length, upon the implementation of the key expansion algorithm. For the initial *AddRound* key abstraction, 6-word round key is sufficient and circumscribed each round with 12 rounds for the encryption of the plain text to cipher text. Expanded key is then metamorphosis into 6 words as key. The remaining of the expanded key is copied as 6 words at a time to form a square matrix. Immediate precedence word *w[i-1]* is needed for each added word *w[i],* with the 6 positions of the word in precedence with *w[i],* as *w[i-6].* This is similar to as exclaimed in for the procedure involved for a block size of 4 words, with a key length of 4 words.

Figure 6 explains the algorithmic procedure involved in the process of KeyExpansion.

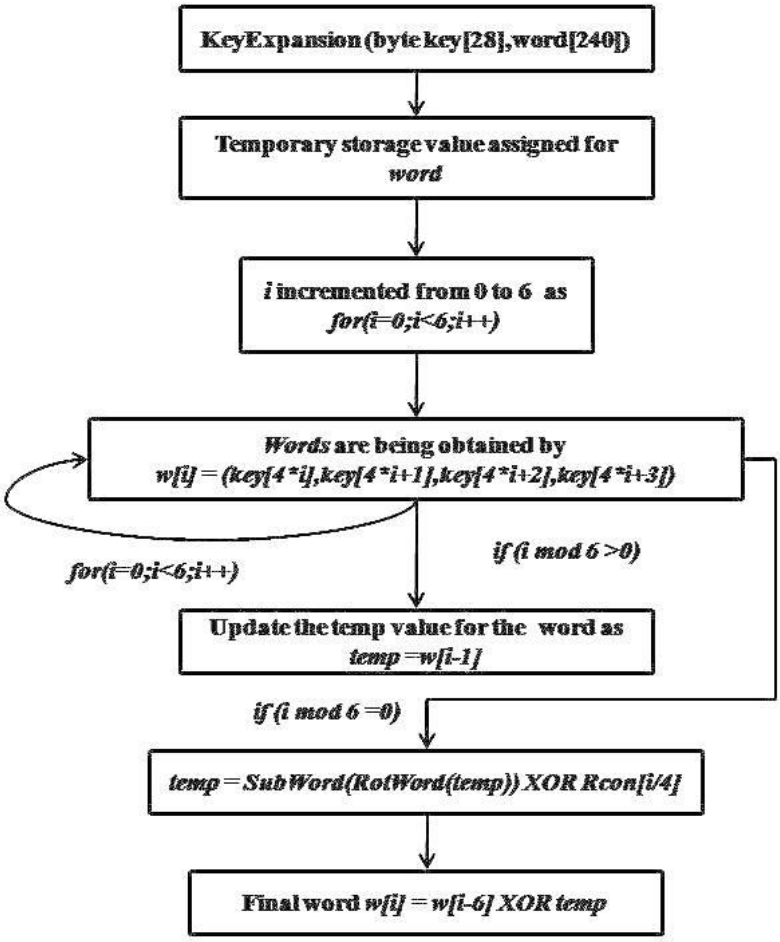


Figure 6. Key expansion algorithm

In the above proposed algorithm, there are three values generated as;

a. *RotWord:* a One-byte circular left shift is done for the word of data considered. So if the input word is [b0 b1 b2 b3 b4 b5 b6] is transformed into data word as [b1 b2 b3 b4 b5 b6 b0] and updated in the temporary register of the word.
b. *SubWord:* The S-box factor is considered here and byte wise substitution is performed on each byte of the input word in the S-box array.
c. *Rcon[j]:* It's a constant with which the word from the temporary register is XORed with and the obtained value is updated in the temporary register as a word. This is called as Round Constant. This is a word with the rightmost bytes in this word with the magnitude 0. The XOR operation performed in the procedure involves a word of data XORed with the constant value, with the XOR operation performed only on the left byte of the word.

The round constant for each round is defined by the equation,
$Rcon[j] = (RC[j], 0,0,0)$, where
$RC[1] = 1$ & $RC[j] = 2 * RC[j-1]$, *j* is the number of rounds.

The constants are multiplied over with the field factor GF($2^6$), where

$m(x) = x^6 + x^5 + x^4 + x^3 + 1$, is taken as the field polynomial.

The Table 1 shown below has the corresponding values as the round constants depending upon the number of rounds the algorithm progresses to encrypt a plain text of an image. Since we process for 12 rounds, we consider the values till *j=12.* The values given in the Table 1 are in hexadecimal format and is as;

Table 1. Values of Round Constants

| *j* | *RC[j]* |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 4 |
| 4 | 8 |
| 5 | 10 H |
| 6 | 20 H |
| 7 | 40 H |
| 8 | 80 H |
| 9 | 1B H=100H |
| 10 | 36 H=200H |
| 11 | 6C H=400H |
| 12 | D8 H=800H |

The formation of the array structure during the execution of the KeyExpansion algorithm in the proposed work will be similar to the expansion array structure as shown in Figure 7. The below figure is for the KeyExpnsion involving 128 bits of key length and data length with *Nk=4, Nb=4* and *Nr=10.*

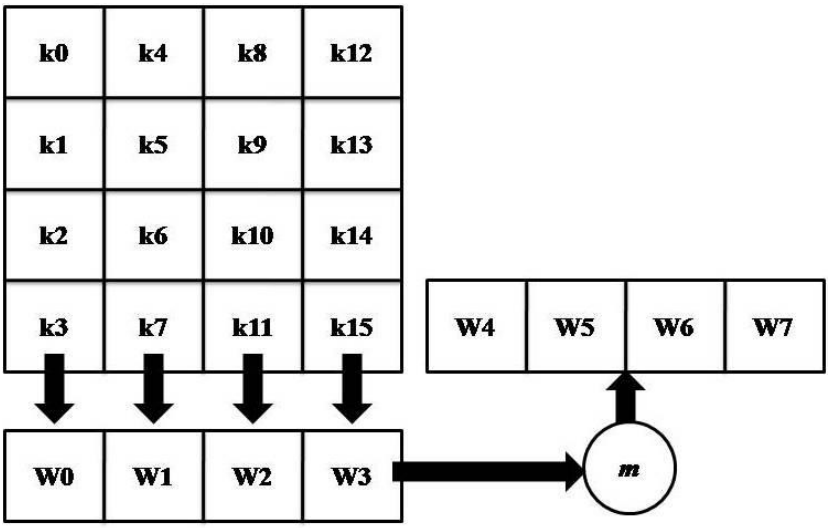


Figure 7. Array structure formed during the keyexpansion algorithm

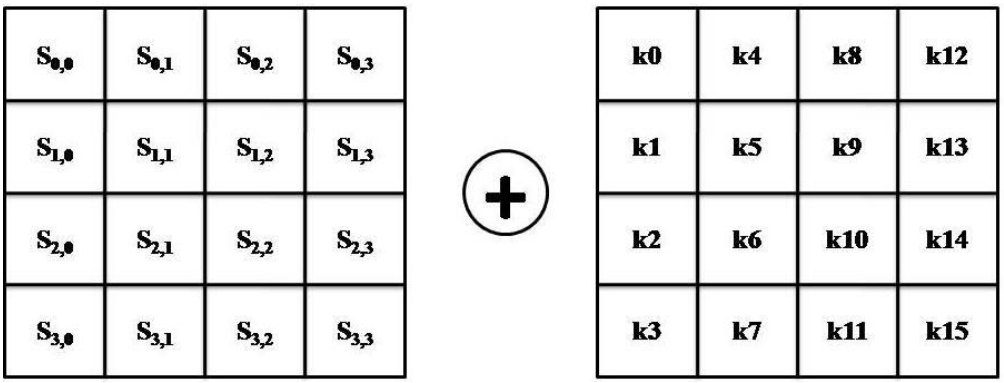


Figure 8. State array and Keyword XOR operation

The consecutive step following the KeyExpansion abstraction in the encryption process is, *SubByte Transformation.*

a. **Modular inversion in GF ($2^6$ ):** This stage is to compute $B(x)=A^{-1}(X)$ for a 6-bit input word (in GF ($2^6$) where $m(x) = x^6 + x^5 + x^4 + x^3 + 1$, is taken as a field polynomial; {OO} is mapped to itself).
b. **Affine Transformation**: This sub-step is performed in GF (2) and defined by. $D(x)=\delta*B(x) \phi C(x)$ where b={1F}=$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, for the encryption process and b={4A}=$x^6 + x^3 + x$ for the decryption.

Working in the composite field, multiplicative inverse is leisured. However, forth and back, we have to map elements in GF ($2^k$) into GF $(2^n)^m$ where k=mn. Therefore both transform and inverse transform matrices are needed. For example, elements in GF ($2^8$) can be mapped to element in GF $(2^4)^2$ by using the polynomial $r(x)=x^2 + x + \beta^{14}$ where $\beta^{14}$ denotes the element in GF($2^4$) of which $I(x)=x^4 + x + I$ is the primitive irreducible polynomial.

The array of the byte values, in the form of a 16 X 16 matrix, in the S-box, is supposed to contain a vivid permutation for all the combination of the 8-bit binary values, with 256 combinations. In this process the new bytes generated before the mapping process are arranged in the State array in a way such that the MSB of the byte of data can be used as to represent the row value and the LSB bit values of the byte of data represents the column value. These representations of the row and the column values are necessary as they assign the indexes into the S-box and ensure the selection of the unique data value of 8-bits. The substitution of the bytes of word in the S-box are updated and ensured for the rows of the S-box array to be transformed circularly. This step cyclically shifts each byte in each row of the state to the left by a predetermined amount. The standard AES algorithm does not shift any bytes in the first row, shifts each byte in the second row left by one byte, shifts each byte in the third row left by two bytes, and shifts each byte in the fourth row left by three bytes. This ensures that each column of the output will have elements of each column of the input. Following

Figure *9* shows shift row transformation. In this process, the first row of the array of the S-box remains unaltered while the circular left shift are performed byte-wise from the second row. The process proceeds as, 1-byte shift for second row, 2-byte for the third and 3-byte for the fourth row. This is formed as shown in

Figure *9*.

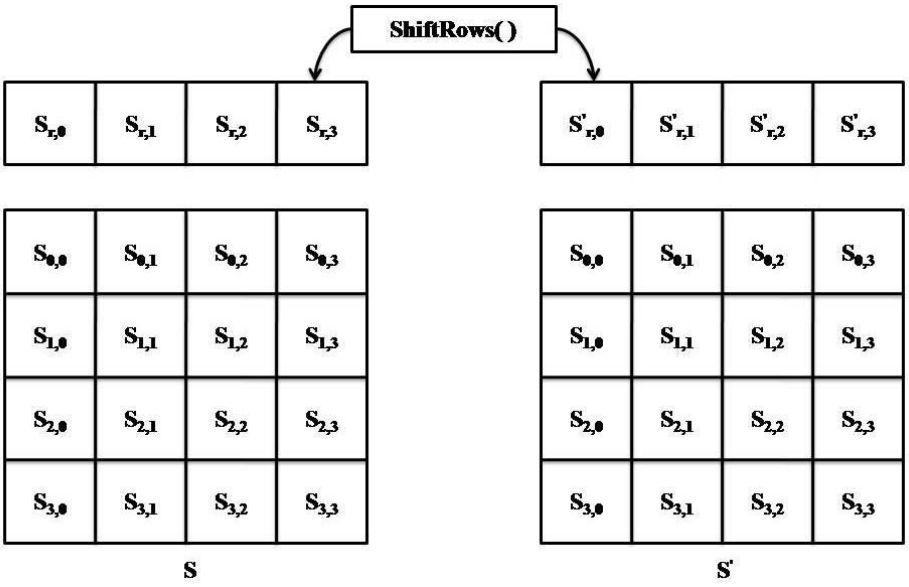


Figure 9. ShiftRow transformations

After all the transformation procedures, each column is operated individually, wherein the value of each byte in an individual column is required to be mapped and replaced with the

transformed new value, the new value representing the function of all the four bytes of data of the column. This operation is performed on the State array, obtained with the multiplicative operation performed on the State array matrix as given in the

Figure *10*. Sum of products of the persisting elements of an individual row and column, represented as individual elements in the product matrix. The elements of the matrix array are subjected to operations of addition and multiplication which are performed for the elements in GF ($2^8$).

$$\begin{bmatrix} 01 & 00 & 01 & 01 \\ 00 & 01 & 00 & 01 \\ 01 & 01 & 01 & 01 \\ 00 & 00 & 00 & 01 \end{bmatrix} \begin{bmatrix} C_{0,0} & C_{0,1} & C_{0,2} & C_{0,3} \\ C_{1,0} & C_{1,1} & C_{1,2} & C_{1,3} \\ C_{2,0} & C_{2,1} & C_{2,2} & C_{2,3} \\ C_{3,0} & C_{3,1} & C_{3,2} & C_{3,3} \end{bmatrix} = \begin{bmatrix} C'_{0,0} & C'_{0,1} & C'_{0,2} & C'_{0,3} \\ C'_{1,0} & C'_{1,1} & C'_{1,2} & C'_{1,3} \\ C'_{2,0} & C'_{2,1} & C'_{2,2} & C'_{2,3} \\ C'_{3,0} & C'_{3,1} & C'_{3,2} & C'_{3,3} \end{bmatrix}$$

Figure 10. MixColumn procedure

This transformation of MixColumn for a single column $j$ ($0 \leq j \leq 3$) of the State array is as,

$$S'(0,j) = (2.s(0,j)) \oplus (3.s(1,j)) \oplus (s(2,j)) \oplus (s(3,j))$$
$$S'(1,j) = (s(0,j)) \oplus (2.s(1,j)) \oplus (3.s(2,j)) \oplus (s(3,j))$$
$$S'(2,j) = (s(0,j)) \oplus (s(1,j)) \oplus (2.s(2,j)) \oplus (3.s(3,j))$$
$$S'(3,j) = (3.s(0,j)) \oplus (s(1,j)) \oplus (s(2,j)) \oplus (2.s(3,j))$$

This above expressions yields the product matrix for the transformation as,

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Thus the iterative process is continued and proceeds to finalize with all the 12 rounds and will yield us with an effective encrypted image as shown in figure Figure 11.

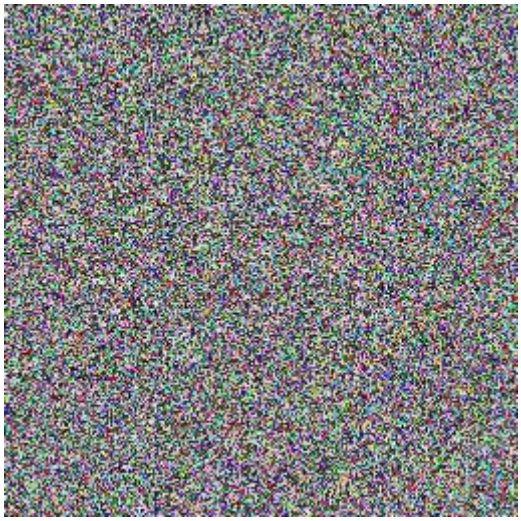

Figure 11. Encoded Shuffled Image

## 7. Analytical Results

An efficient encryption algorithm is proven with its effectiveness it the algorithmic approach provides a valuable analytical values substantiating the process that defines the algorithm against the brute-force attacks. Various metrics such as histogram analysis, time analysis and correlation coefficient analysis are discussed in this section to substantiate the proposed image encryption scheme. These analytical results are liable to prove that the proposed cryptosystem is more secure.

### 7.1 Correlation Coefficients Analysis

The analysis of the pixels which are vertically as well as horizontally yields in the correlation analysis in a plain image and also in the encrypted image. The correlation coefficients of the original image and the encrypted image is calculated using the expression,

$$C_r = \frac{N \sum_{j=1}^{N}(x_j * y_j) - \sum_{j=1}^{N} x_j * \sum_{j=1}^{N} y_j}{\sqrt{\left(N \sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) * \left(N \sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right)}}$$

In the above expression,

*N* – Total number of pixels of selection in the image input to the algorithmic machine

*x* & *y* – value of the adjacent pixels in the image within a block-set.

In our proposed algorithm, after the substituting the respective values of the variables the correlation coefficient values were obtained,

Table 2. Correlation Coefficient Values

| *File Description & Type* | *Size* | *Correlation Coefficient* |
|---|---|---|
| *Original, Grayscale* | *256 X 256* | *0.007786* |
| *Encrypted, Grayscale* | *256 X 256* | *-0.008124* |

The correlated images are thus obtained as shown in **Error! Reference source not found.**.

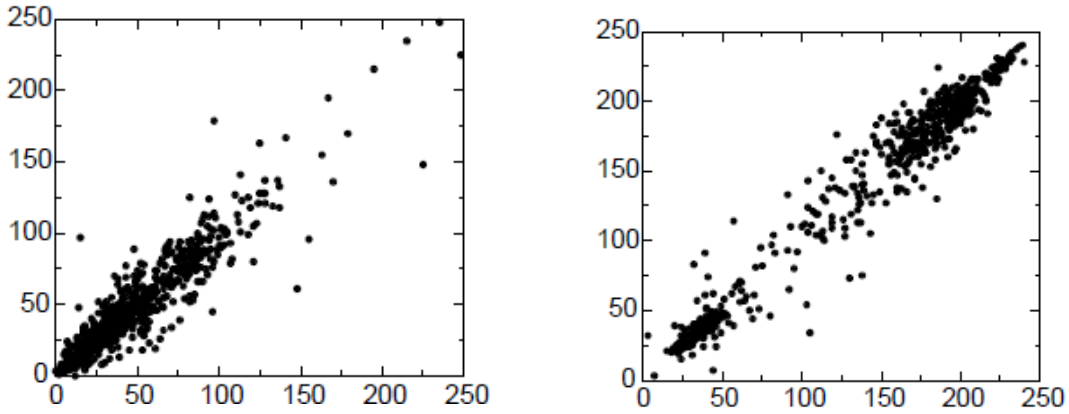


Figure 12. Correlation of two adjacent pixels horizontally and vertically for encoded image

The probability plot for the correlated coefficient value in-terms of its magnitude is also plotted. The maximum value of probability is obtained as 0.95, an equivalent to 95%. Thus the original image is highly correlated to the encoded image. The probability plot is as shown in Figure *13*.

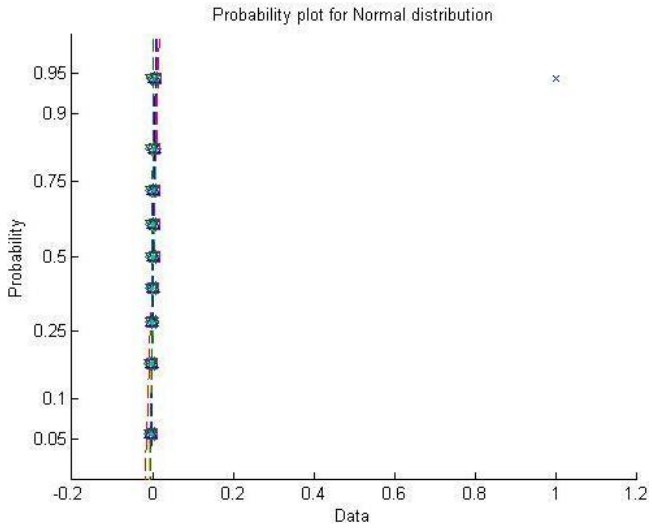


Figure 13. Probability plot of the normally distributed correlated values

### 7.2 Histogram Analysis

The analytical observation which describes the distribution of the image pixels on the magnitude of their number, graphically at the particular intensity values. The histograms of the original image before its encryption and the shuffled images obtained from the original images as well as the encoded shuffled images and the decrypted shuffled images. We can observe from the plots of the histograms that they are uniform for the original and the shuffled images. The histogram plots for the procedures are given in Figure *14* & Figure 15.

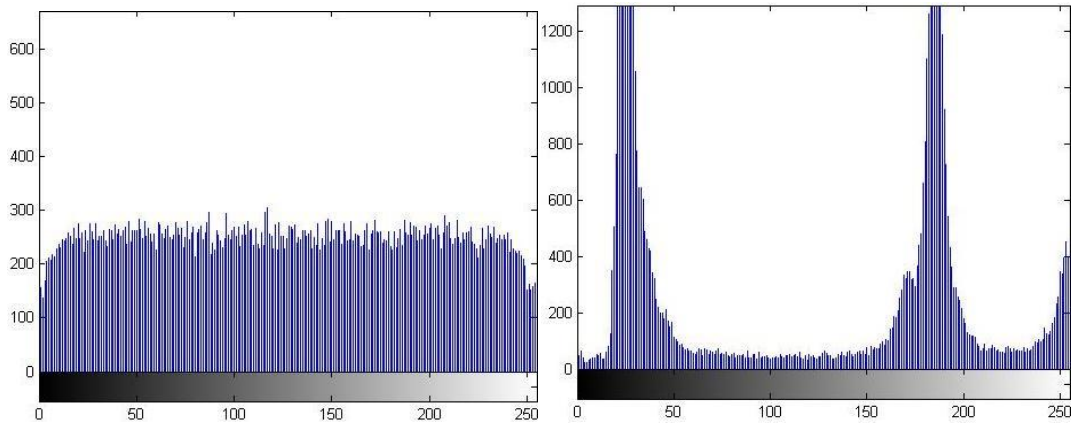


Figure 14. Histogram of the original & the encoded image

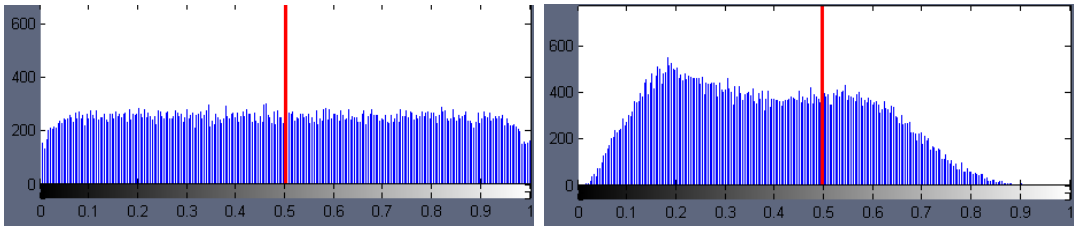


Figure 15. Shuffled original & encoded image histogram

We can also observe from the above figures that the histogram plot of the original image and the encoded/encrypted images, for both original as well as the shuffled images are significantly different and are not the same on realistic values, proving that they are insusceptible to any kind of statistical as well as brute-force attacks. This also proves that the proposed work and the efficiency orbiting the algorithm.

### 7.3 Time Analysis

The execution speed of the algorithm and the rate at which the algorithm runs and encrypts the image of consideration using the proposed encryption scheme was analyzed being run on a machine with the configuration Intel Quad Core Processor (3rd Gen) with 2GB RAM machine. The elapsed time for the analysis is referred to this and is given in Table 3. Time consumed for Encryption & Decryption process

Table 3. Time consumed for Encryption & Decryption process

| Image Size (pixels) | Pixels | Encryption/ Decryption Time (s) |
|---|---|---|
| 256 X 256 | 32 pixels | 0.046904 (Encryption) |
| 256 X 256 | 32 pixels | 0.044016 (Decryption) |

## 8. Conclusion

The information or the data within an image, which of a DICOM format medical standard, possess certain confidential data whose integrity is to be maintained during its transmission over varying bandwidths and also during the storage of such data. The proposed algorithm in this literature provides an efficient and an effective approach, wherein the medical standard DICOM format image is first shuffled using the 2D CAT Mapping algorithm. Thus obtained shuffled image which will be input to the AES Encryption. In this proposed process of encryption we have 4 major transformation functions which are iterative and the number of rounds of iterations depends upon the secret key size given in terms of bits. The secret key size is considered as 192 bits while the data size is also accommodated as 192 bits. This algorithm

for the process of AES Encryption is iteratively run for 12 rounds to obtain the encrypted image. Thus this procedure makes the encrypted data/image more robust and uncompromising against any statistical attacks. The key of 192 bits is more robust which averages for the encryption at a very effective rate of encryption and decryption process. The analytical procedures were carried out as Histogram Analysis, Correlation Coefficient Analysis and Time Analysis, which parameterize the effectiveness and the robustness of the proposed image encryption/decryption process. The proposed procedure profound to be more effective for real-time, medical process, and data-realistic applications, wherein the data/image needs to be transferred/transmitted, stored across bandwidths and across various applications wherein the shared data access is required with data confidentiality at a high priority and necessity.

## References


[1] Shivaputra, HS Sheshadri, V Lokesha. "An Efficient Lossless Medical Image Compression Technique for Telemedicine Applications". *Computer Applications: An International journal (CAIJ).* 2015; 2(1): 63-69, ISSN: 2393-8455.

[2] Shivaputra, HS Sheshadri, V Lokesha. "An Exquisite Approach for Image Compression Technique using Lossless Compression Algorithm for ROI & Non-ROI Regions". *International Journal of Computer Science, Information technology and Control Engineering (IJCSITCE)*. 2015; 2(1/2): 1-13, ISSN: 2394-7527.

[3] Sesha Pallavi, Indrakanti Associate, PS Avadhani. "Permutation based Image Encryption". *International Journal of Computer Applications*. 08/2011, 28(8), DOI: 10.5120/3404-4748.

[4] M Zeghid, M Machhout, L Khriji, A baganne, R Tourki. "A Modified AES Based Algorithm for Image Encryption". *International Journal of Computer, Control, Quantum and Information Engineering*. 2007; 1(3): 726 - 731.

[5] Mohammad Ali Bani Younes, Aman Jantan. "Image Encryption Using Block-Based Transformation Algorithm"l *IAENG International journal of Computer Science*. 35:1, IJCS_35_1_03, February.

[6] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, Ganapati Panda. "Image Encyrption using Advanced Hill Cipher Algorithm". *International Journal of Recent Trends in Engineering*. 2009; 1(1): 663 - 667.

[7] Prachi Junwale, R Manasa Annapurna, G Sobha. "A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm". *International; Journal of Advanced Research in Computer Science and Software Engineering*. 2013; 3(11): 614- 618.

[8] Bibhudendra Acharya, Sarat Kumar Patra, Ganapati Panda. "A Novel Cryptosystem Using Matrix Transformation". Proceedings of *SPIT-IEEE Colloquium & International Conference*. 2008; 4: 92-95.

[9] Zhang Yun-Peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, Dai Wei-di. "Digital Image Encryption Algorithm based on Chaos and Improved DES". *IEEE International Conference on Systems, Man and Cybernetics*, ISSN: 1062-922X, ISBN: 978-1-4244-2793-2, 474-479.

[10] Benyamin Norouzi, Seyed Mohammad, Seyedzadeh, Sattar Mirzkuchaki, Mohammad Reza Mosavi. "A novel Image Encryption based on Hash Function with only Two-Round Diffusion Process". *Multimedia Systems*. ISSN: 0942-4962, DOI 10.1007/s00530-013-0314-4.

[11] Ismail Amr Ismail, Amin Mohammed, Hossam Diab. "A Digital Image Encryption Based - A Composition of Two Chaotic logistic Map". *International Journal of Network Security*, 01/2010, DOAJ.

[12] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani. "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption". *IEEE, International Conference on Electronics and Information Engineering (ICEIE 2010).* ISBN: 978-1-4244-7681-7.

[13] Gamil RS Qaid, Sanjay N Talbar. "Bit-Level Encryption and Decryption of Images using Genetic Algorithm: A New Approach". *IPASJ International Journal of Information technology (IIJIT)*. 2013; 1(6), ISSN: 2321-5976.

[14] Verma OP, Hanmandlu M, Sultania AK. A Novel Fuzzy Ant System for Edge Detection. 2010 IEEE/ACIS 9th *International Conference on Computer and Information Science*. 2010: 228–233.

[15] Musheer Ahmad, M Shamsher Alam. "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping". *International Journal on Computer Science and Engineering*. 2009; 2(1): 46-50.

[16] ZH Guan, F Huang, W Guan. "Chaos-based Image Encryption Algorithm". *Physics Letters A*. 2005; 346(1-3): 153-157.

[17] NK Pareek, Vinod Patidar, KK Sud. "Image Encryption using Chaotic Logistic Map". *Image and Vision Computing*. 2006; 24: 926-934.

[18] Mayank Mishra, Prashanth Singh, Chinmay Garg. "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping". *International Journal of Information and Computation Technology*. 2014; 4(7): 741-746, ISSN: 0974-2239.

[19] Gamail RS Qaid, Sanjay N Talbar. "Encryption and Decryption of Digital Image Using Color Signal". *IJCSI International Journal of Computer Science Issues*. 2012; 9(2-2): 588-592.
[20] K Sakthidasan, BV Santhosh Krishna. "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images". *International Journal of Information and Education Technology*. 2011; 1(2): 137-141.
[21] Pia Singh, Prof Karamjeet Singh. "Image Encryption and Decryption Using Blowfish Algorithm in MATLAB". *International Journal of Scientific & Engineering Research*. 4(7): 150-154, ISSN: 2229-5518.
[22] Nithin N, Anupkumar M Bongale, GP Hegde. "Image Encryption based on FEAL Algorithm". *International Journal of Advances in Computer Science and Technology (IJACST)*. 2013; 2(3): 14-20, ISSN: 2320-2602.
[23] S Dey. SD-EI: A Cryptographic Technique to Encrypt Images. In Proc. Of *IEEE international conference in Cyber Security, Cyber Warfare and Digital Forensic*. 2012: 28-32.
[24] R Sharma. A Novel Approach to combine Public-key encryption with Symmetric-key encryption. *The International Journal of Computer Science & Applications.* 2012; 1(4): 8-15.