# An Integrated Algorithm Supporting Confidentiality and Integrity for Secured Access and Storage of DICOM Images

**Suresh Jaganathan** *whosuresh@gmail.com*
*Assistant Professor*
*Department of Computer Science and Engineering*
*Sri Sivasubramania Nadar College of Engineering,*
*Chennai, Tamilnadu, India*

**Arun Fera M** *fera26@gmail.com*
*PG Scholar*
*Department of Computer Science and Engineering*
*Sri Sivasubramania Nadar College of Engineering,*
*Chennai, Tamilnadu, India*

**Abstract**

In healthcare industry, the patient's medical data plays a vital role because diagnosis of any ailments is done by using those data. The high volume of medical data leads to scalability and maintenance issues when using health-care provider's on-site picture archiving and communication system (PACS) and network oriented storage system. Therefore a standard is needed for maintaining the medical data and for better diagnosis. Since the medical data reflects in a similar way to individuals' personal information, secrecy should be maintained. Maintaining secrecy can be done by encrypting the data, but as medical data involves images and videos, traditional text based encryption/decryption schemes are not adequate for providing confidentiality. In this paper, we propose an algorithm for securing the DICOM format medical archives by providing better confidentiality and maintaining their integrity. Our contribution in this algorithm is of twofold: (1) Development of Improved Chaotic based Arnold Cat Map for encryption/decryption of DICOM files and (2) Applying a new hash algorithm based on chaotic theory for those encrypted files for maintaining integrity. By applying this algorithm, the secrecy of medical data is maintained. The proposed algorithm is tested with various DICOM format image archives by studying the following parameters i) PSNR - for quality of images and ii) Key - for security.

**Keywords:** Medical Images, DICOM, Encryption, Healthcare, Confusion, Diffusion, Message Digest

## 1. INTRODUCTION

Patient's data plays a major role in the healthcare industry where the data is used for diagnosis of any ailments. Nowadays digital form of storing them replaced the traditional film based medical images. Storing them on-site (within the hospital network) is not an efficient solution for current and future trend because of issues such as scalability, and interoperability. Therefore there must be an off-site management of the patient's data. These medical data are in image and video formats such as i) CR (Computed Radiography)images, ii) CT (Computed Tomography) images, iii) MR (Magnetic Resonance) images and iv) PET (Positron Emission Tomography) images etc. Since they need to be communicated to experts across the world to diagnose and to take decisions for treatment, some standard format must be followed for maintaining and transferring which led to the development of DICOM (Digital Imaging and Communications in Medicine) standard. This standard includes the format for maintaining the medical data in (.dcm) format [1, 2].

The main concern regarding the medical data is the confidentiality. Since the medical data involves patients data it must be kept secretly like an ATM pin number. Health Insurance

Portability and Accountability Act (HIPAA) [1] is an act in US that tells about how secure the patient's medical data should be. In future it is sure that all the countries will bring out the same kind of act and is mandatory to protect the data. Many such security issues come in picture such as, confidentiality, authentication, authorization and integrity [3]. All these issues must be considered while providing security to the medical data. The confidentiality is provided by encrypting the medical data before they are stored in off-site. Unlike text messages, image data has special features such as high redundancy, bulk capacity which generally make encrypted image data vulnerable to attacks via cryptanalysis. Because of high correlation among pixels, directly treating image data as ordinary data for encryption will make file format conversion impossible. Usually these images are huge in size, which together makes traditional encryption methods difficult to apply and slow in process. Hence in this case, content encryption, where only the image data are encrypted, leaving file header and control information unencrypted is preferable. In addition to confidentiality, integrity also must be maintained for the medical data since they are stored off-site.

Two general principles that guide the design of cryptographic ciphers are diffusion and confusion [4]. Diffusion means spreading out the influence of a single plain-text digit over many cipher text digits, so that the statistical structure of the plain-text becomes unclear. Confusion means using transformations that complicate the dependence of the statistics of the cipher text on the statistics of the plain-text. They are closely related to the mixing and ergodicity properties of chaotic maps [5].

Rest of the paper is organized as, Section 2 explains some of the related work done. Section 3 provides details about the chaotic cat map employed for providing confusion. Section 4 provides details of improved chaotic cat maps which provide diffusion along with confusion. Section 5 gives a brief explanation of proposed hash algorithm for providing integrity. Section 6 explains the architecture of the proposed algorithm for securing the medical images. Experimental results for the proposed algorithm are presented in Section 7, and at last, Section 8 concludes the work with references.

## 2. RELATED WORK

In [3], a hash algorithm is discussed based on logistic chaotic map whose first round input value acts as a key. It is compared with the MD5 algorithm and proved that it is better for image data.
In [6], the encryption method for image data is based on confusion and diffusion where the confusion is carried out by any kind of chaotic map like Arnold, Baker map etc and diffusion is carried out by a XOR based function. In [15], a parametric hashing algorithm that is invariant to encryption by allowing a small part of the statistical signature of the original image to emerge despite the encryption process is developed. In [17], the diffusion function is carried out with modulo operation since the inverse is very difficult to find. An attack to image encryption using chaotic cat map is possible once if the key values are known to the adversary and known-image attack is the one which commonly occurs in case of key theft [19].

## 3. CHAOTIC CAT MAP

### 3.1 Usage of Confusion

Confusion is one of the important aspects of cryptography. Confusion is meant for confusing the statistical attackers to derive the original data from the statistics of the cipher data. The high initial-value sensitivity and ergodicity properties of chaotic map are very essential in providing confusion for medical image data. Advantages of using confusion are i) Sensitivity to initial conditions and control parameters and ii) pseudo-randomness and ergodicity. Also it has some disadvantages they are i) after the period of the cat map is reached, the original image appears and ii) once the key parameters are leaked, the adversary can easily decrypt the cipher data. In the confusion process, many different 2D chaotic maps are used, such as the Baker map, the Cat map and the Standard, which must be used to realize the confusion of all pixels [5]. Some of the 3D maps currently in practice are just extensions of 2D chaotic maps [7].Even chaotic maps can provide integrity. Chaotic maps properties are in close relation with the cryptosystem security. First, its parameter is used as confusion key. The higher the parameter sensitivity is, then higher the key sensitivity and the stronger the cryptosystem. Secondly, the initial-value sensitivity and state ergodicity of the chaotic map determine the confusion strength. In chaotic confusion process, initial value refers to the initial position of a pixel. Thus, the higher the initial-value sensitivity is, then smaller the correlation between adjacent pixels and the more random, the confused image. Similarly, state ergodicity means that a pixel in certain position can be permuted to any position with the same probability. Thus, the higher the state ergodicity is, then more random the confusion process and the more difficult the statistic attack [8]. Therefore, the chaotic map with high initial-value sensitivity and state ergodicity is preferred [9]. Other than this chaotic theory other encryption schemes for images are T-matrix and watermarking [10]. In [11], it is proved that chaotic based image encryption works efficiently than traditional AES based encryption. In [12], chaos based encryption is done with the help of traditional wavelet transform.

### 3.2 Mathematical Details [Confusion]

Let (X, d) be a metric space. Then a map f is said to be (Devaney) chaotic on X if it satisfies the following conditions:

- f exhibits sensitive dependence upon its initial conditions
- f is topologically transitive

The dependence on initial conditions is very important in chaos as it makes hard to determine long term behavior of dynamical systems which show signs of chaos. If a chaotic output is generated by one set of initial conditions and then if it is changed with a little number of bits, then the output will change drastically. As mentioned previously, chaos is sometimes seen as meaning of random or unstable, but it is important to make sure that the randomness also exhibits the conditions from the definition of chaos [13].

The Arnold Cat Map is a discrete system [14] that stretches and folds its trajectories in phase space [15] as shown in the equation 1.

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N \tag{1}$$

where $x_{i+1}$ and $y_{i+1}$ are the pixel positions of the cipher image, $x_i$ and $y_i$ are the pixel positions of original image, N is the number of columns considered while applying the cat map.
The values *p* and *q* indicate the parameters which must be kept secret and act like the key values. One more important condition of cat map is that it must be area preserving. To achieve this, the determinant value should be 1 so that the reverse operation can be applied [16].

## 4. IMPROVED CHAOTIC CAT MAP

### 4.1 Diffusion

Due to some of the demerits of confusion, we go for diffusion. Diffusion [17] is another important aspect of cryptography which aims at providing additional security. In our proposed system, diffusion is done for the data that is got from the process of confusion. For diffusion function, a change of a pixel can spread to other pixels, which keeps the cryptosystem of high plain-text sensitivity. (0, 0) is the first pixel position in normal scan mode, which cannot be permuted by chaotic maps. So by applying diffusion process, the first pixel is always changed by addition operation with diffusion key$Q_{i-1}$. If a change happens in a pixels gray-level, then the change can cause great ones in other pixels through diffusion process [18]. Thus, the greater the changes caused by diffusion process are, then higher the cryptosystem plaintext sensitivity and the more difficult the systems security against differential attack [19].

### 4.2 Mathematical Details [Diffusion]

The relationship between the first pixels plaintext $\mathrm{P}_0$, diffusion key $Q_1$and cipher text$Q_0$ is

$$Q_0^n = [D(P_0, Q_{-1})]^n \tag{2}$$

where D () is the diffusion function. A powerful diffusion function is given in equation 3,

$$Q_i = P_i \oplus (4 * Q_{i-1} * (1 - Q_{i-1})) \tag{3}$$

where $\mathrm{P}_i$ is the current plain text pixel, $\mathrm{Q}_i$ is the current cipher text pixel and $Q_{i-1}$ is the initial value of diffusion process which is used as a key for diffusion process. Here the second term in the formula is a kind of logistic cat map which also provides pseudo randomness. Since we use a XOR operation which considers each and every bit of the input pixel value, it brings a stronger security by making the statistical relation among the plain images and the cipher images. Advantages of using Diffusion are i) since we use a kind of logistic map for diffusion, it provides a random behavior so that a tiny change in the plain image is reflected in more than one pixel in the cipher image [20] and ii) Pseudo-randomness and ergodicity. Disadvantages are i) usually the diffusion function takes some time to complete its operation because the real valued arithmetic operation consume much computation time and ii) once the key parameters are leaked, the adversary can easily decrypt the cipher data.

## 5. PROPOSED HASH ALGORITHM

The hash algorithm is mainly used for providing integrity. Generally a hash function takes a variable length data as input and produces a fixed length output hash value [15]. One main aspect of hash algorithm is that it must be injective i.e. any two inputs should not result in same hash values. Since patients' medical data are of our primary concern, distortion of them may lead to wrong diagnosis and even threaten patients' life. Traditional methods like MD5, SHA etc can be used to generate hash values. But since images don't fit themselves as good candidates for traditional hash algorithms [3], a new direction has emerged in calculating hash for images. It led to calculating hash based chaotic theory which deals with dynamic systems. Some chaotic maps like logistic maps are a kind of irreversible map [3] which does not produce original data after getting reversed. This algorithm makes full use of every bit in an image file to generate initial vector and to control the digesting process. The proposed hash algorithm involves both traditional methods and chaotic map and is discussed in Section 5.

## 6. ARCHITECTURE OF PROPOSED ALGORITHM

Figure 1 shows the architecture of our proposed algorithm. The proposed algorithm uses both confusion and diffusion properties of cryptography. DICOM standard is used for both storing and exchanging the medical files such as scan images. By applying confusion and diffusion to the DICOM format medical images, their confidentiality is maintained. The keys used for confusion and diffusion must be known only to authorized persons. Some methods are proposed based on confusion for providing confidentiality but they are vulnerable to known plain image attack since confusion only rearranges the pixels. This algorithm is against the known plain image attacks when diffusion is applied. The proposed approach takes two parts 1) encrypting/decrypting the medical files 2) calculating hash values. Both the parts are done with some mathematical equations which represent the chaotic based theory.

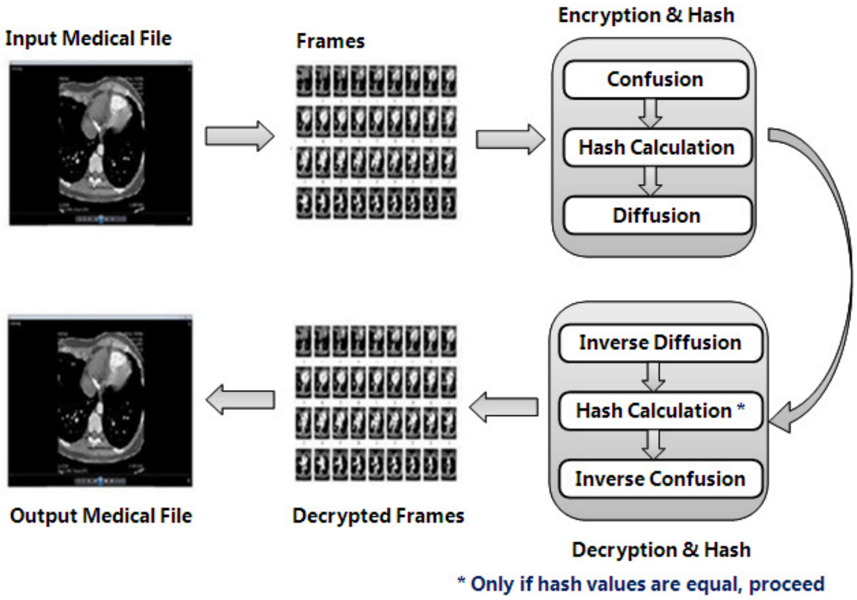

**FIGURE 1**: Architecture of the proposed algorithm

## Part 1: Encryption

- Convert the DICOM file into a video sequence using third party software. e.g.: Rubo DICOM viewer
- The video file is converted to individual frames
- Extract the pixel coordinates starting from the left top for all the frames
- Apply the formula to perform confusion

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \mod N$$

where $x_{i+1}$ and $y_{i+1}$ are the pixel positions of the cipher image, $x_i$ and $y_i$ are the pixel positions of original image, N is the number of columns considered while applying the cat map

- Apply the below formula to perform diffusion

$$Q_i = P_i \bigoplus (4 * Q_{i-1} * (1 - Q_{i-1}))$$

where $P_i$, is the current plain text pixel, $Q_i$ is the current cipher text pixel and $Q_{i-1}$ is the initial value of diffusion process which is used as a key for diffusion process

## Decryption

- Apply the formula to perform inverse diffusion

$$P_i = Q_i \bigoplus (4 * Q_{i-1} * (1 - Q_{i-1}))$$

where $P_i$, is the current plain text pixel, $Q_i$ is the current cipher text pixel and $Q_{i-1}$ is the initial value of diffusion process which is used as a key for diffusion process

- Apply the formula to perform inverse confusion

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} pq+1 & -p \\ -q & 1 \end{pmatrix} \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} \mod N$$

where $x_{i+1}$ and $y_{i+1}$ are the pixel positions of the cipher image, $x_i$ and $y_i$ are the pixelpositions of original image, N is the number of columns considered while applying the cat map

- From the pixel values, construct the frames
- Convert the individual frames to a video file

**Part 2: Hash algorithm**

- The output of confusion process is applied to hash algorithm because calculating hash after diffusion will lead to collision due to the property of diffusion function.
- For each individual images of the DICOM file:
  i) Calculate SHA-512 for the image which produces a128 byte message digest
  ii) Divide 128 bytes into eight 16 bytes
  iii) Calculate XOR for the nearest pairs so that four outputs are obtained
  iv) For each of those four outputs, apply the logistic map as in equation 4, four times with the key parameter as the values obtained from the previous step

$$x_{n+1} = y_{n+1}\,(1 - x_n) \tag{4}$$

where $y_{n+1}$ is the current plain text pixel, $x_n$ is the previous hash value and $x_{n+1}$ is the current hash value. After iterating through all pixels the lastly obtained hash
value is provided to next step
v) Concatenate the results from the previous step
vi) Apply MD5 for the obtained value which is the final hash value of the image containing 32 digit hexadecimal numbers.

## 7. EXPERIMENTAL RESULTS

The proposed improved chaotic cat map algorithm is applied to various DICOM format image archives and tests are conducted. The results are verified with PSNR values for QoS and with key for security.

Peak Signal to Noise Ratio (PSNR) is used as a quality parameter for reconstruction of compression images or videos. Here signal is in the original data and the noise is in the compressed data. Calculating PSNR values by using equations 5 and 6 is used as estimation to human awareness for reconstructing quality of compressed data or encrypted data. Two steps are involved in calculating PSNR values.

*PSNR Calculation:*

Step 1: Calculate Mean Square Error [MSE]

$$d(f(x,y), f^{`}(x,y)) = ||(f(x,y) - f^{`}(x,y)||^{2}$$

$$= \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j}^{n-1}\left((f(i,j) - f^{`}(i,j)^{2}\right), \tag{5}$$

where $f(x,y)$ and $f^{`}(x,y)$ original and reconstructed images respectively, *m* and *n* are image size.

Step 2:

$$\mathrm{PSNR} = 10\log_{10} {}^{1}/_{MSE} \tag{6}$$

Figure 2 shows the test DICOM file (FEROVIX) used in this paper for evaluating the proposed algorithm.

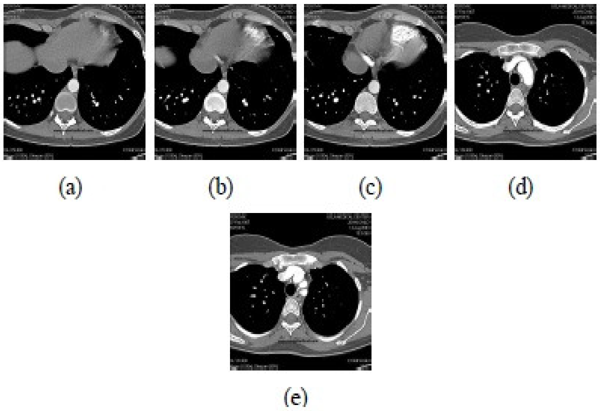

**FIGURE** 2: Sample Test Sequence

Sample test images are taken from a DICOM file which contain details of *Ferovix* CT scan images e.g. Lungs. These test images (shown in Column 1 of Figure 3) are encrypted using Arnold Chaotic Cat Map and its results are shown in Figure 3. When the images are encrypted using Arnold Chaotic Cat Map, the pixels are rearranged. Hence a shuffled image is obtained as input (shown in Column 2 of Figure 3).Images are encrypted using the key (1,1). If the key value is changed, the original is not obtained which is shown in Column 3 of Figure 3.

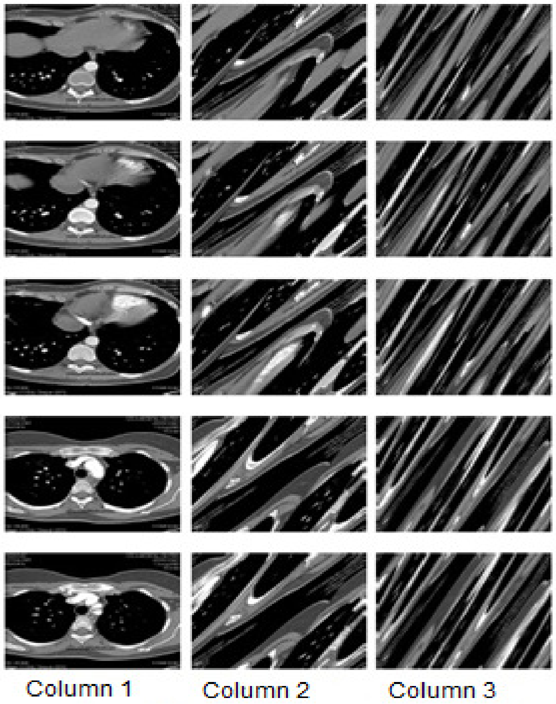

**FIGURE 3:** Applying Chaotic Cat Map

As stated earlier, applying Chaotic Cat Map only is not enough for security and is vulnerable to crypt-analysis. Hence the diffusion is applied with confusion, which makes the crypt-analysis harder, hence improved security. Figure 4 shows the image sequences after applying confusion (Column 2 of Figure 4) and diffusion (Column 3 of Figure 4).

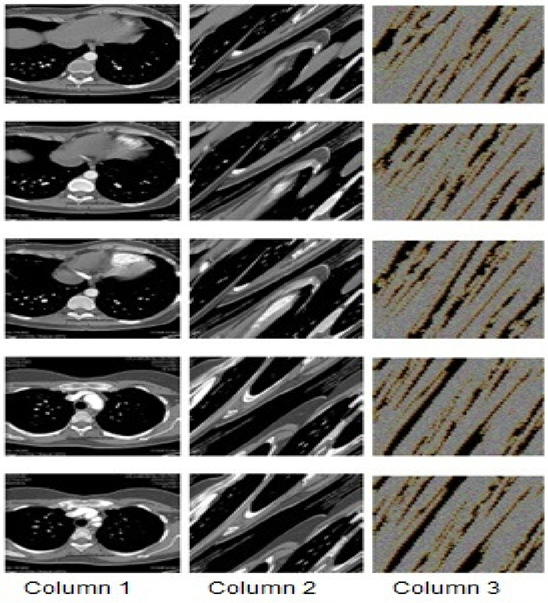

**FIGURE 4:** After applying proposed algorithm [Confusion and Diffusion]

Tested DICOM image sequences are encrypted with the available chaotic cat map algorithm and also with the proposed algorithm i.e. applying both confusion and diffusion. Table 1 shows the PSNR values obtained to check the viewable quality of DICOM images after decryption for confusion and after applying the proposed algorithm i.e. both confusion and diffusion. When confusion is applied to the image, the pixels values are rearranged when applying inverse operation, some pixels are not rearranged properly hence, there is a decrease in PSNR value (shown in blue color (bottom) in Figure 5), when applying only diffusion the pixels value are changed and there is no rearrange of pixels and when doing inverse operation the original image is obtained, hence increase in PSNR value (shown in red (top) in Figure 5).

When applying the proposed algorithm i.e. combination of confusion and diffusion, the viewable quality of image after decryption comes in between two extremes (shown in green color (middle) in Figure 5), having quality viewable image reproduction.

| Bit rate [kb] | Confusion | Diffusion | Proposed Algorithm |
|---|---|---|---|
| | [dB] | [dB] | [dB] |
| 350 | 33.83 | 42.99 | 38.41 |
| 360 | 33.26 | 42.6 | 37.93 |
| 380 | 33.35 | 42.6 | 37.97 |
| 390 | 33.14 | 42.35 | 37.74 |
| 400 | 32.94 | 39.06 | 36 |

**TABLE 1:** PSNR Comparison for various algorithms

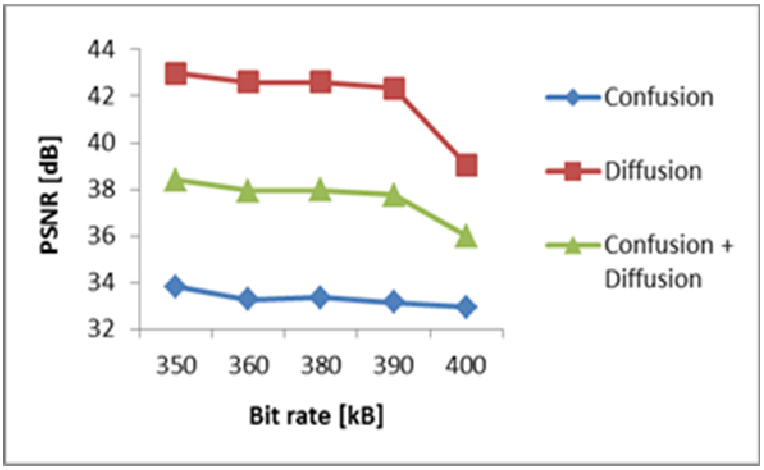

**FIGURE.5:** Graph showing PSNR values for various algorithms

The proposed hash algorithm is applied to various DICOM format image archives and tests are conducted. The results are verified by changing the bits in the image so that even a single bit change in the image leads to a different hash value. The results show that collision does not occur among different images and also the results have proved that.Research result shows that, because of the inherent characteristics of Chaos Maps and Hash function lead to the simplicity, high sensitivity to initial conditions and good performance of our algorithm.

Table 2 shows the message digests generated by the DICOM images taken under study and also after applying confusion.

| Hash Value<br>DICOM images | Hash Value<br>After confusion |
|---|---|
| dbfba83ff1532c94d90d85dfe2de828b | 91bb4fefe246308a17d16e36efd9e587 |
| e665305217c723a3cf3802310eacf2ee | 0b81f3066191ead6b18337baec6f9741 |
| 3ad46f25268952bdfa17e6a1d1786df7 | 5802f25d5bece1e741cd12c363cecc50 |
| 1697cb8ba4c40858fd152414fc3daebd | 7d280caca60b370f0b182b268e62a377 |
| e2a64ec5b8a1db0401c026ef938e5e65 | 5b25d654e9beb5589a09f503b770c128 |

**TABLE 2:** Message digests for various images

Table 3 shows the message digest generated by the DICOM images taken under study along with the message digest generated if any random bit is changed in the image got after applying confusion.

| Hash value for<br>DICOM images | Hash value<br>After one bit change |
|---|---|
| dbfba83ff1532c94d90d85dfe2de828b | 2781b4fb71b0ebb7bcea1ef776c425c7 |
| e665305217c723a3cf3802310eacf2ee | b37e49729158afdd8d0e1539adc387a1 |
| 3ad46f25268952bdfa17e6a1d1786df7 | da52e005b51377ca7f3fae35f7dad744 |
| 1697cb8ba4c40858fd152414fc3daebd | c20931bf34df388fa71211b4149faa47 |
| e2a64ec5b8a1db0401c026ef938e5e65 | 159513702c1b5452ddcdc98fb8bd777b |

**TABLE 3:** Message digests for various images

The average rate of bits changed (P) is given by equation 7,

$$P = (B/128)*100 \quad (7)$$

where B is the average number of bits changed while a random bit gets changed due to some attack or modification by unauthorized person. Table 4 shows the individual values of P for the images that are taken in study. The average rate of bits changed (P) is 52.80 for all those images. Since the hash algorithm relies on each and every bit of the image, the resulting message digest is very hard to find and also to infer the plain text from the message digest.

| **Input Image in column 2 of FIGURE 3** | **Number of bits changed in resultant image out of 128 when random bits are changed in input image** | **Rate of change of bits** |
|---|---|---|
| Image 1 | 68 | 53.12 |
| Image 2 | 69 | 53.9 |
| Image 3 | 65 | 50.78 |
| Image 4 | 70 | 54.68 |
| Image 5 | 66 | 51.56 |

**TABLE 4:** Average rate of changed bits

## 8. CONCLUSION

In this paper we proposed a new algorithm for providing two fold securities for maintaining the confidentiality and integrity of patient's medical data. Confusion is provided by means of Arnold Cat Map and diffusion is provided by means of a strong diffusion function. By employing this algorithm, we found that this algorithm suits well for medical images and is tested for QoS with PNSR and security level with keys. Integrity is provided by means of combining traditional hash algorithms with logistic cat map. Future work entails in storing the DICOM medical archives in cloud environment due to their large size and maintaining the authenticity by means of providing certificates to authorized users.

## 9. REFERENCES

[1] Chia-Chi Teng, Jonathan Mitchell, Christopher Walker, Alex Swan, Cesar Davila, David Howard, Travis Needham (2010), ”A Medical Image Archive Solution in the Cloud”. IEEE, 10.1109/ICSESS.2010.555234 3, pp 431-434

[2] Suresh Jaganathan, M B Geetha Manjusha, 2011, “dFuse: An Optimized Compression Algorithm for DICOM-format image archive”, International Journal of Biometrics and Bioinformatics (IJBB), Volume (5) ,Issue (2) , 42-52, ISNN: 1985-2347

[3] Zhiliang Zhu, KeZhai, Beilei Wang, Hongjuan Liu, Huiyan Jiang (2009) ”Research on Chaos-based Message Digest Method for Medical Images”. IEEE, 1109/CISP.2009.5301139, pp 1-510

[4] LjupEoKocarev, GoceJakimoski, Toni Stojanovski, Ulrich Parlit (1998), ”From chaotic maps to encryption schemes”, Circuits and Sys tems, 1998. ISCAS 98. Proceedings of the 1998 IEEE International Symposium. 10.1109/ISCAS.1998.698968, vol.4, pp 514 – 517.

[5] YUAN-BIAO ZHANG, ”Chaos based cryptography. An alternative to algebraic cryptography”.2008.

[6] Yaobin Mao and Guanrong Chen (2005), ”Chaos-Based image encryption”. www.open-image.org/725publication/journal/CBIE.pdf

[7] Guanrong Chen, Yaobin Mao b, Charles K. Chui (2003) ”A symmetric image encryption scheme based on 3D chaotic cat maps”. Science Direct, doi:10.1016 / j.chaos.2003.12.022.

[8] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law (2006),"A Fast Image Encryption Scheme based on Chaotic Standard Ma p". Cryptography and Security conference cited as arXiv:cs/0609158v1 , Volume 372, Issue 15, pp 2645-2652.

[9] Ling Bin, Liu Lichen, Zhang Jan (2010) "Image encryption algorithm based on chaotic map and S-DES".IEEE ,10.1109/ICACC.2010. 5486998, pp 41-44.

[10] Monisha Sharma (2010), "Image encryption techniques using chaotic schemes: A review". International Journal of Engineering Science and Technology Vol. 2(6),2359-2363, ISSN: 0975-5462, pp 1-10.

[11] Muhammad Asim and VarunJeoti,(2007) "Image Encryption: Comparison between AES and a Novel Chaotic Encryption Scheme" I EEE. 10.1109/ICSCN.2007.350697, pp 65-69.

[12] Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng (2010), "A Chaos-Based Image Encryption Algorithm Using Wavelet Transform" IEEE , 10.1109/IEMBS.2010.5628061, pp 1037-1040.

[13] De wang, Yuan-biaozhang (2009) "Image encryption algorithm based on s-boxes substitution and chaos random sequence". International Conference on Computer Modeling and Simulation, DOI 10.1109/ICCMS.2009.26.

[14] Gabriel Peterson (1997), Arnolds Cat Map, Math 45 Linear Algebra, Fall 1997.

[15] Kashyap, S.; Karthik, K. (2010) "Authenticating encrypted data". IEEE, 10.1109/NCC.2011.5734696, pp 1-5.

[16] Katherine Struss (2009) "A Chaotic Image Encryption". Spring, Mathematics Senior Seminar, 4901.

[17] ShiguoLian, Jinsheng Sun, Zhiquan Wang (2005) "Security analysis of a chaos-based image encryption algorithm". Science direct, Physica A: Statistical Mechanics and its Applications 351 (2-4) , pp 645-661.

[18] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law (2006) "A Fast Image Encryption Scheme based on Chaotic Standard Map". Cryptography and Security conference cited as arXiv:cs/0609158v1 , Volume 372, Issue 15, pp 2645-2652.

[19] ShuaiRen, ChengshiGao, Qing Dai, XiaoFeiFei (2010) "Attack to an Image Encryption Algorithm based on Improved Chaotic Cat Maps".3rd International Congress on Image and Signal Processing (CISP2010), 10.1109/CISP.2010.5647659, pp 533-536.

[20] Kwok-Wo Wong, Bernie Sin-Hung Kwok,(2007) "An Efficient Diffusion Approach for Chaos-based Image Encryption". 3rd International conference Physics and Control (Physcon 2007)