Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 8 (2023) pp: 05-15
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Encryption of Digital Images using Hyperchaotic 6D System and its application in Healthcare

Anannya Chuli
SCOPE
Vellore Institute of Technology Vellore, India

Shashwat Kumar
SCOPE
Vellore Institute of TechnologyVellore, India

Tamizharasi T
SCOPE
Vellore Institute of TechnologyVellore, India

Abstract**—***In the era of information technology, consumers have to send millions of photographs back and forth on a daily basis. It's crucial to secure these pictures. It is a common practiceto secure image content using digital image encryption. Using secret keys, digital images are transformed into noisy images in image encryption techniques, and the same keys are needed to restore the images to their original form. The majority ofimage encryption methods rely on two processes: confusion and diffusion. This research presents a brand-new technique for image encryption that makes use of a hyper-chaotic system and aFibonacci Q-matrix. This technique, which makes use of the six- dimension hyper-chaotic system's randomly generated numbers, confuses the original image. The Fibonacci Q-matrix was then utilized to dilute the permuted image. The suggested picture encryption technique was examined utilizing sensitivity, key space, histograms, and data cut and noise attacks. Additionally, the performance of the suggested method was evaluated againsta number of other algorithms utilizing entropy, correlation coef- ficients, and robustness against assault. The suggested approach performed better than the current picture encryption algorithms and attained an excellent security level.*

Keywords**—***Image Encryption, Decrytpion, Cyber Security, Chaos Theory,*

R*eceived 01 August, 2023;* ***R****evised 08 August, 2023;* ***A****ccepted 11 August, 2023 © The author(s) 2023.* ***P****ublished with open access at* ***www.questjournals.org***

I. INTRODUCTION

The multimedia shared and stored over the Internet is mostly in the form of images. Hence, the confidentiality and authentic- ity of digital images are ensured by means of image encryp- tion. Image encryption finds its applications in many fields such as medical imaging, telemedicine, business, biometric authentication, and military communication. Numerous image encryption techniques have been presented to meet these se- curity constraints, including digital water-marking techniques,image scrambling methods, image steganography, and image cryptography. In the last few decades, the exploitation of chaos in cryptography has shown a surge in interest due to its fundamental property of sensitivity to initial conditions leadingto data sets, which while deterministic, give the appearance of randomness.

Thousands of digital photos are transmitted every second during the ordinary operation of digital image transmission over multiple networks. Users of social networks do not want other people to have access to their photographs. Medi- cal images are sensitive in healthcare networks, where their improper use could result in incorrect diagnosis and poor medical judgment. High-security levels are needed when trans- mitting military photographs via various networks to avoid unauthorized access. Digital picture owners typically do not want unauthorized access to their images. These factors have made protecting the information in photos a crucial concern. Image confidentiality is achieved through a variety of securitymeasures, making it impossible

for an unauthorized person to view the content of an image. The three primary categoriesof picture security techniques are data concealing, image watermarking, and encryption. A hidden message is inserted into the cover image using data-hiding techniques so that it cannot be seen. When using picture watermarking techniques, digital data is introduced into the image at points where the original and watermarked versions may both be seen. In picture encryption methods, the key used to convert the digital input image to a noisy image cannot be predicted or comprehended. Without the key, users cannot restore the encrypted image.

II. LITERATURE REVIEW

Ø Cosine-transform-based chaotic system for image encryp-tion.

In a chaos-based encryption scheme, the security level relies strongly on the complexity of its used chaotic map. However, existing chaotic maps may exhibit drawbacks in different aspects. Firstly, existing chaotic maps may demonstrate chaos degradation when they are implemented in finite precision plat-forms, as their output states cannot be distributed uniformly. Secondly, they do not have complex behaviors, making their trajectories easily predicted using certain technologies. More- over, their chaotic ranges are either narrow or discontinuous. If a chaotic map has narrow or discontinuous chaotic ranges, its chaos properties may be destroyed when its parameters are disturbed by certain external factors such as noise. Reports have indicated that several image encryption schemes using existing chaotic maps may be successfully attacked.

Ø Encryption using 2D Hénon-Sine map DNA approach.

This paper first proposes a two-dimensional Hénon-Sine map (2D-HSM). The new map possesses better ergodicity andpseudo-randomness, and its parameters have a wider chaotic range, compared with many existing chaotic systems. Then a DNA encoding and a DNA exclusive-or (XOR) operation rule are defined because the DNA approach applied in image encryption can greatly improve the efficiency of image permu-tation and diffusion. A novel image encryption scheme whose image pixels are diffused by the DNA approach and permu- tated by 2D-HSM is proposed to protect image content while an image is transferred over the Internet. Some experimental analyses such as statistical attack analysis, differential attack analysis, exhaustive attack analysis, robustness against noise, and computational complexity have been applied to measure the new scheme, and the experimental results illustrate the scheme possesses better encryption performances than that of other references, and therefore, is secure in real-world communication.

Ø Image encryption scheme based on chaotic tent map.

The chaos-based cryptographic algorithms have suggested some new and efficient ways to develop secure image en- cryption techniques. Image encryption systems based on such map show some better performances. Firstly, the chaotic tent map is modified to generate a chaotic key stream that is more suitable for image encryption. Secondly, the chaos-based key stream is generated by a 1-D chaotic tent map, which performsbetter in terms of randomness properties and security level. The performance and security analysis of the proposed image encryption scheme is performed using well-known ways. The results of the fail-safe analysis are inspiring, and it can be concluded that the proposed scheme is efficient and secure.

Ø Color image encryption based on hybrid hyper-chaotic system and cellular automata.

Cellular automata is a self-organizing structure with a setof cells in which each cell is updated by certain rules that aredependent on a limited number of neighboring cells. The majordisadvantages of cellular automata in cryptography include a limited number of reversal rules and the inability to produce long sequences of states by these rules. In this paper, a non-uniform cellular automata framework is proposed to solvethis problem. This proposed scheme consists of confusionand diffusion steps.In the confusion step, the positions of the original image pixels are replaced by chaos mapping. The key image is created using non-uniform cellular automata and then the hyper-chaotic mapping is used to select random numbers from the image key for encryption. The main contribution ofthe paper is the application of hyperchaotic functions and non- uniform CA for robust key image generation. Security analysis and experimental results show that the proposed method has a very large key space and is resistive against noise and attacks. Ø Image encryption using a synchronous permutation-diffusion technique.

A synchronous permutation and diffusion technique is de- signed in order to protect gray-level image content while sending it through the internet. To implement the proposed method, a two-dimensional plain-image is converted to one dimension. Afterward, to reduce the sending process time,permutation and diffusion steps for any pixel are performed simultaneously. The permutation step uses a chaotic map and deoxyribonucleic acid (DNA) to permute a pixel, while diffusion employs a DNA sequence and DNA operator to encrypt the pixel. Experimental results and extensive security analyses have been conducted to demonstrate the feasibility and validity of this proposed image encryption method.

Ø Image encryption and hiding algorithm based on com- pressive sensing and random numbers insertion.

The paper proposed a new meaningful image encryption al-gorithm based on compressive sensing and information hidingtechnology, which hides the existence of the plain image and reduces the possibility of being attacked. Firstly, the discrete wavelet transform (DWT) is employed to sparse the plainimage. This is followed by a confusion operation on pixel positions, where the logistic-tent map is employed to produce a confusion sequence. And then the image is compressed and encrypted by compressive sensing to form an intermediate cipher image. Here, the measurement matrix is generated using a low-dimension complex tent-sine system. To further enhance recovery quality, we suggest that the intermediate cipher image be filled with random numbers according to the compression ratio and confusing them to obtain the secret image. Finally, two-dimensional (2D) DWT of the carrier image is performed, followed by singular value decomposition. The singular values of the secret image are embedded into the singular values of the carrier image with certain embedding strength to obtainthe final visually meaningful encrypted image.

Ø A new color image encryption using a combination ofthe 1D chaotic map.

The algorithm introduces a method of making a simple and effective chaotic system by using a difference of the output sequences of two same existing one-dimension (1D) chaotic maps. Simulations and performance evaluations show that the proposed system is able to produce a one-dimension (1D)chaotic system with better chaotic performances and larger chaotic ranges compared with the previous chaotic maps. To investigate its applications in image encryption, a novel encryption system of linear-nonlinear-linear structure based on total shuffling is proposed. The experiment demonstrated the accuracy of the encryption algorithm. Experiments and security analysis prove that the algorithm has excellent per- formance in image encryption and various attacks.

Ø A novel plaintext-related image encryption scheme using a hyper-chaotic system. In this scheme, we used the classical encryption architecture: permutation and diffusion. The initial conditions of the hyper-chaotic Lorenz system which is em- ployed in permutation and key stream generation algorithms are generated by information from the original image and initial key. Therefore, the encryption process has a strong relationship with the plain images in the proposed scheme. So, our work performs excellently in resisting the known-plaintext attack. In addition, the results of many widely used security analyses and comparisons with other works show that ourwork has outstanding security performance for digital image communication.

Related works have some constraints that can be summa- rized as follows:

1. The initial conditions get low keyspace and less sensitiv- ity.
2. The initial condition of the chaotic map does not depend on the plain image which leads to weaknesses in resisting the various differential attacks.
3. When the encrypted image gets attacked with noise and data cuts, some of the encryption algorithms were unable to retrieve the plain image.
4. Some of these algorithms were unable to resist statistical attacks as the histogram of the encrypted image is not flat.

The contributions of this work are summarized as:

1. We are the first ones to utilize the Fibonacci Q-matrix inimage encryption.
2. We are the first ones to use a 6D hyperchaotic system inimage encryption.
3. The integration of the 6D hyperchaotic system and the Fibonacci Q-matrix assures high-security level.
4. The proposed algorithm has a large keys-pace that leadsto good resistance to brute force attacks.
5. The proposed image encryption algorithm has superrobustness to most attacks.
6. The analysis of the obtained results from the proposedalgorithm showed excellent performance.

III. OBJECTIVE AND NOVELTY

The vast majority of image encryption techniques depend on the confusion and diffusion processes. This study introduces a novel hyper chaotic system-based and Fibonacci Q-matrix- based image encryption method. This method confuses the original image by using randomly generated numbers from the six-dimension hyperchaotic system. The permuted image was then diluted using the Fibonacci Q-matrix. Sensitivity, keyspace, histograms, data cut, and noise assaults were used to analyze the proposed picture encryption method. Additionally, using entropy, correlation coefficients, and resilience against attack, the performance of the proposed approach was com- pared to that of a number of different algorithms. The recom-mended method outperformed the existing photo encryption techniques and obtained a very high level of security.

Among the objectives of the work are:
1. The Fibonacci Q-matrix is used for image encryption
2. Use of the 6D hyperchaotic system for image encryption.
3. The 6D hyperchaotic system and Fibonacci Q-matrix areto be integrated to ensure a high-security level.
4. The suggested algorithm offers strong resistance to bruteforce assaults due to its huge key space.
5. The suggested approach for picture encryption is to beextremely resistant to most attacks.

Compared to other related works, this work holds up betterbecause:
1. It has more sensitivity to the starting conditions and lowkeyspace.
2. The chaotic map's initial state is independent of the plainimage, which makes it less resilient to differential attacks.

3. Some encryption techniques were unable to recover the plain image when the encrypted image was subjected to noise and data cuts which is not the case with this work.
4. Because the histogram of the encrypted image is not flat, very little of encryption techniques are vulnerable to statisticalattacks.

IV. WORKFLOW AND ALGORITHM

In order to prevent unwanted access, relevant information must be transformed into an unrecognizable form using cryp- tography. The picture content has a number of important properties, including high redundancy, space, capacity, and thecorrelation of the bit pixels. These qualities necessitate the useof some sort of encryption method, the main goal of which is to protect the privacy of the image while it is being transmitted. Confusion and dispersion are the two phases that make up the encryption. In each of these procedures, the arrangements and values of the pixels are altered. The 6D hyper chaotic system is the foundation of the confusion step. The system's starting state, which is based on the plain picture, is first calculated. The hyper chaotic system is then iterated to produce a new vector, after which we choose three sequences.The diffusion process is carried out to acquire the encrypted picture after confounding the plain image. The Fibonacci Q-matrix serves as the foundation for the diffusion in our algorithm.

In other words, the relevant actual information is hidden by using an encryption method to convert the plain image into a cipher image. The image may be safely transferred over the network by being encrypted, making it hard for unauthorized individuals to decipher it. At the receiving end of the network, a decryption technique is used to convert the encrypted pictureback into the original image.

A decryption technique must be employed to decode the encoded picture in order to restore the original image whenan image is encrypted. While an encrypted picture is com- bined with a key for image encryption, an encrypted imageis combined with a key for image decryption. In order tocreate chaotic systems-based cryptography algorithms for safe picture encryption and communication in the presence of an attacker, there has been a lot of research and development in these fields.

V. METHODOLOGY

The close correlation between chaotic systems and cryp- tography has resulted in a greater number of cryptographic algorithms being formulated on the chaos that can protect images and communications when attackers are present. Chaos theory is the study of complex, typically non-linear systems that exhibit quickly changing irregular and frequently unex- pected behavior. These systems are very sensitive to beginning circumstances and state changes and feature complex inter- actions, mixing, non-periodicity, and feedback loops. Chaos theory and the science of encryption are combined in equal measure to form chaotic cryptography. The primary distinction

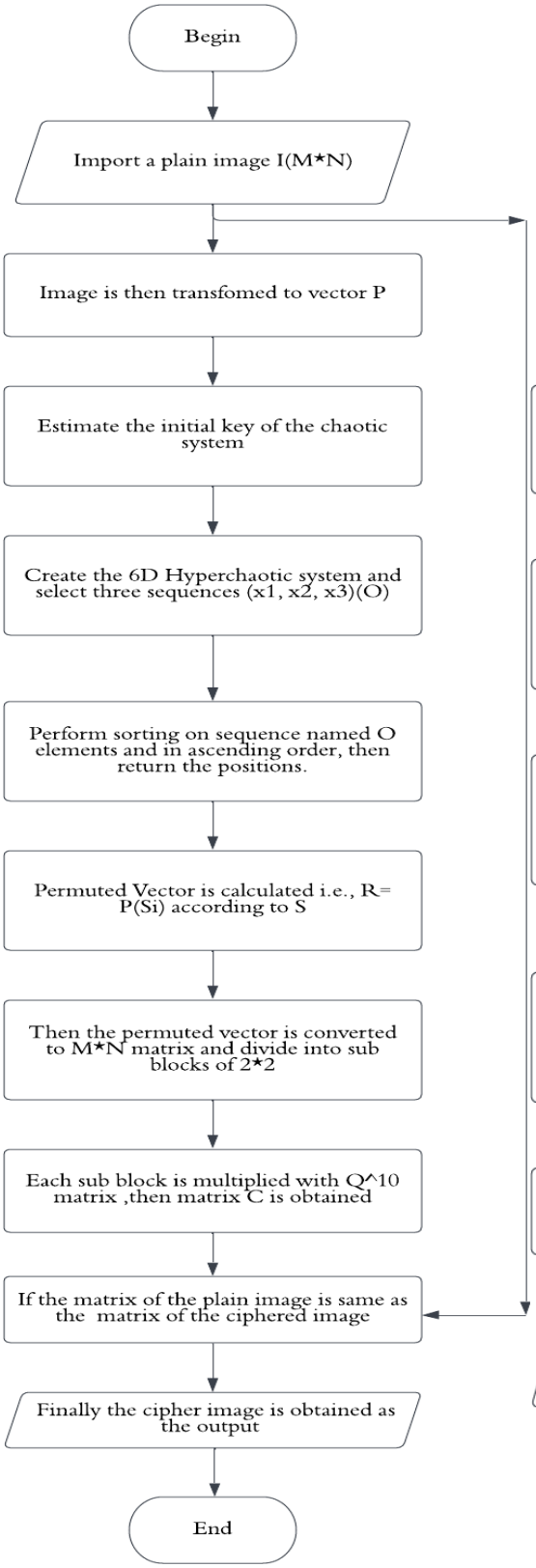

Fig. 1. Encryption Process

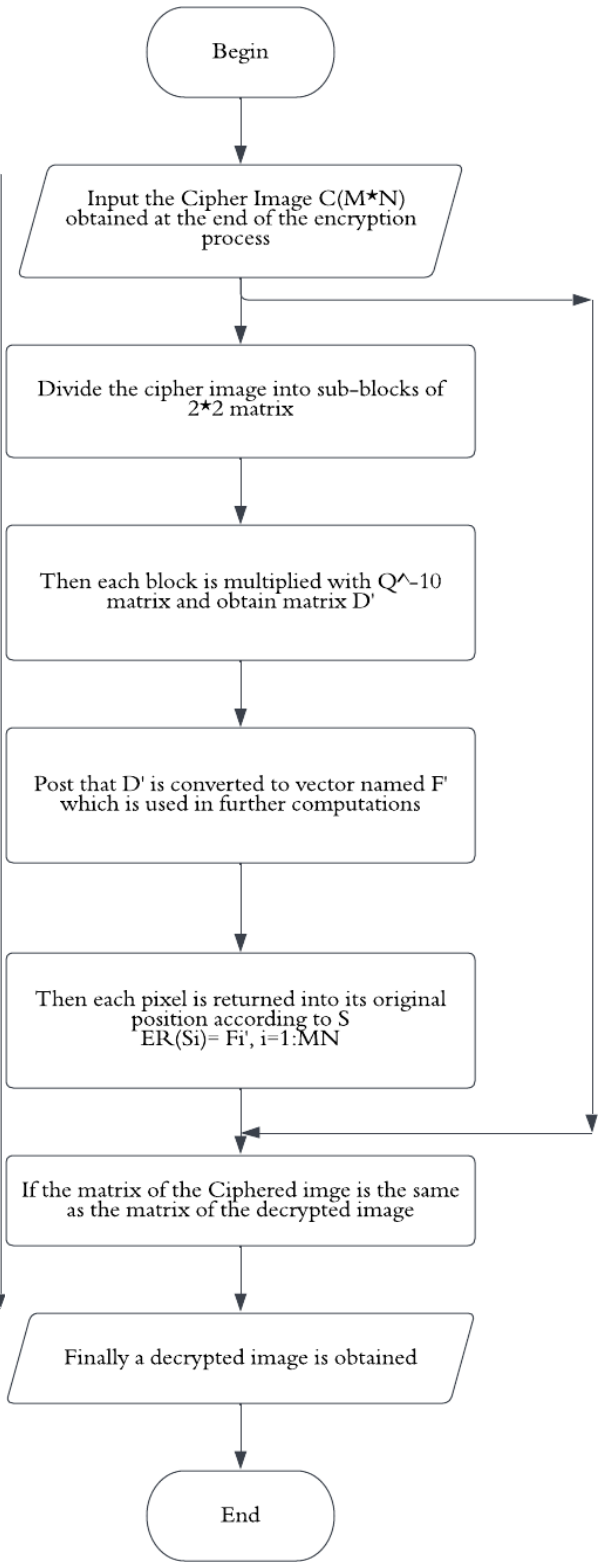

Fig. 2. Decryption Process

between the two is that whereas cryptosystems are mapped on an infinite set of integers, chaotic systems are defined on real numbers. Traditional ciphers like AES and DES work well for text encryption but are ineffective for picture cryptography because of the repeating data that pixels in related images display. This problem is solved by chaos-based encryption methods, which generate uniformly dispersed random keys that cover the picture data in the cipher images.

Chaotic systems demand in-depth knowledge of the entire system since they are sensitive to beginning circumstances and measurement accuracy. We frequently lack the characteristics and state representation necessary to fully understand how complex interactions and changes occur in chaotic systems. Continuous model training, assessment, and monitoring is a straightforward concept that is crucial to machine learning in general. Iterative processes should be used for complicated changing systems' predictive analytics. Training a new system in the future is helpful because Chaos Theory specifically highlights the unpredictable nature of chaotic systems over extended horizons, or in the future.

Hyperchaotic systems can display complicated dynamical characteristics despite having a relatively basic algebraic structure. It features a unique equilibrium over a wide range of parameters and a hyperchaotic attractor with four positive Lyapunov exponents, which is of special interest. The presence of the hyperchaotic and chaotic attractors is confirmed by a numerical study of phase trajectories, Lyapunov exponents, bifurcation, power spectrum, and Poincare´ projections. In addition, two comprehensive mathematical characterizations for 6D bifurcation are evaluated, and the stability of the hyperbolic equilibrium is also examined.

The new algorithm utilized a 6D hyperchaotic system and Lucas matrix to encrypt the input image. Since the 6D hyperchaotic system has complex high-dynamic behaviors and two positive Lyapunov exponents, its utilization improves the encryption performance and increases the security level.

The proposed approach encrypts grayscale images in two phases using a six-dimension (6D) hyperchaotic system and a Fibonacci Q-matrix. First, the 6D hyperchaotic system is used to shuffle the positions of the pixels in the original image. From this 6D hyperchaotic system, just three sequences were randomly chosen to enable the original image. Second, the diffusion process, which is carried out on the sub-blocks of a confused image, makes use of the Fibonacci Q-matrix. Based on completed trials, the suggested image encryption technique successfully and efficiently encodes grayscale images.

The hyperchaotic functions' dynamical behavior is much more complicated than the corresponding one of the low-dimension chaotic functions. A hyperchaotic system should have at least four dimensions. Moreover, low-dimension chaotic functions contain only one positive Lyapunov exponent, while the hyperchaotic systems have at least two.

The encryption depends on two steps: confusion and diffusion. The pixels' arrangements and values are modified in these processes, respectively. The confusion step is based on the 6D hyperchaotic system and it has been defined as follows

$$x_1 = a(x_2 - x_1) + x_4 - x_5 - x_6$$

$$x_2 = cx_1 - x_2 - x_1x_3$$

$$x_3 = -bx_3 + x_1x_2$$

$$x_4 = dx_4 - x_2x_3$$

$$x_5 = ex_6 + x_3x_2$$

$$x_6 = rx_1$$

Where a,b,c,d,e, and rare constants; x_1, x_2, x_3, x_4, x_5, and x_6 refer to state variables of the 6D hyperchaotic system. In this paper, the constant values selected are $a = 10$, $b = 83$, $c = 28$, $d = 1$, $e = 8$, and $r = 3$.

This selection ensures that the system has two positive Lyapunov exponents that achieve the condition (the sum of all exponents is negative)

The algorithm is started by initializing, i=1 and transforming the image array to a vector P.Calculations are performed for generating the initial key of the hyperchaotic system by using the below formula-

$$x_1 = \frac{\sum_{i=1}^{MN} P(i) + (M + N)}{2^{23} + (M + N)}$$

$$x_i = mod(x_{i1}10^6, 1) i = 2, 3, .., 6$$

After calculating the initial conditions (x1, x2, . . . , x6) of the system that is based on the plain image, we then obtain a new vector in N0 + MN/3 times and then discard the N0 values to make a new sequence L with size M × N. In the next step, we select three sequences (x1, x3, and x5) from the system. This vector L is then Sorted in ascending order and their positions returned in vector S is used to confuse the plain image.

Following the confusion process, diffusion is performed using the Fibonacci Q-matrix to obtain the encrypted image. The Fibonacci sequence can be defined in the following way-

The elements of the Fibonacci sequence, Fn, are:

$$F_n = F_{n-1} + F_{n-2}, n > 1$$

where $F_1 = F_2 = 1$.

The Fibonacci Q matrix is expressed as:

$$Q = \begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

The nth power of the Fibonacci Q matrix is the matrix defined by:

$$Q^n = \begin{matrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{matrix}$$

$$Det(Q_n) = F_{n+1}F_{n1} - F_n^2 = (1)^n$$

The inverse matrix Q^{-n} has the following form:

$$Q^{-n} = \begin{matrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{matrix}$$

As a result, P generates a newly shuffled sequence R according to the following formula:

$$R_i = P(S_i),\ i = 1 : MN$$

Using the Fibonacci Q-matrix, the scrambled image sequence R is transformed into the matrix R and divided into two-by-two blocks.The Chipper image C is obtained by multiplying each 2 × 2 sub-block in R with the Fibonacci Q matrix (Q^{-10}) :

$$\begin{matrix} C_{i,j} & C_{i,j+1} \\ C_{i+1,j} & C_{i+1,j+1} \end{matrix} = \begin{matrix} R'_{i,j} & R'_{i,j+1} \\ R'_{i+1,j} & R'_{i+1,j+1} \end{matrix} \begin{matrix} 89 & 55 \\ 55 & 34 \end{matrix} \quad mod 256$$

$$with i = 1 : 3 : \ldots\ldots : M, j = 1 : 3 : \ldots\ldots\ldots N.$$

By assuming I = C then i = i + 1.

Two rounds of confusion and diffusion are replicated and the above steps are performed to get the encrypted image.

The decryption steps are the reverse of the encryption steps. The encrypted image (C) is divided into blocks, each with size 2 × 2, and then the diffusion equation with Q^{10} is applied to image blocks by using the following equation:

$$\begin{matrix} D_{i,j} & D_{i,j+1} \\ D'_{i+1,j} & D_{i+1,j+1} \end{matrix} = \begin{matrix} C_{i,j} & C_{i,j+1} \\ C_{i+1,j} & C_{i+1,j+1} \end{matrix} \begin{matrix} 34 & -55 \\ -55 & 89 \end{matrix} \quad mod 256$$

where i = 1 : 3 : 5 . . . : M; j = 1 : 3 : 5 . . : N. The scrambled image (D) obtained from the previous step is converted into vector W.The vector S generated in the encryption step is used to return each pixel to its original position by the following equation:

$$ER(S_i) = W_i,\ i = 1 : MN$$

Fig. 3. Skull

Convert the vector ER in to matrix to obtain the decrypted image (D).Two rounds of decryption steps are performed to get the decrypted image.

VI. Results and Comparative Study

The suggested approach was evaluated against other picture encryption algorithms. Every experiment was carried out using MATLAB. It is possible to hide the grey information in the original image.

ENTROPY

The entropy of an image can be defined as:

$$H(m) = \sum_{i=1}^{2^w-1} P(m_i) log_2 \frac{1}{P(m_i)}$$

The more disordered the images are, the better the entropy approximates,as it is thought of as a critical index for gauging the randomness of images. The entropy of a few grey photos encrypted with the new and old algorithms has an optimal value of 8 for grey images. The best average entropy value is captured by our suggested methodology.

The average of the entropy values for each size of the images produced by our suggested algorithm is shown in the results table. The outcomes are then contrasted with the approaches. For the chipper photos that were encrypted using the novel technique, all entropy values were close to 8.

The proposed encryption technique yields images with the highest unpredictability. It is demonstrated that the distribution of grey values in encrypted photos is uniform, indicating that the encryption system can successfully fend against malicious attacks.

VII. Applications

Digital images are crucial in developing cutting-edge techniques for remote diagnosis and quicker first aid administration to provide better and quicker health services. These digital images are typically transferred between hospitals, doctors, and patients through public networks, often containing private

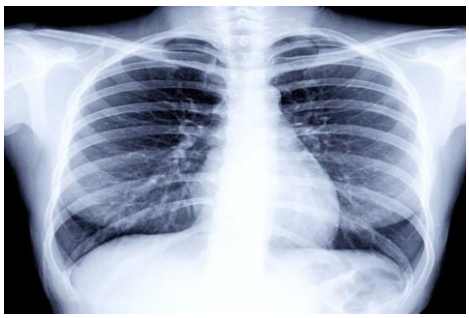

Fig. 4. Plain Image - Ribs

Fig. 5. Plain Image - Hand

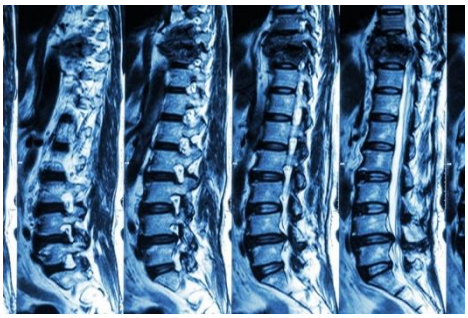

Fig. 6. Plain Image - Spine

Fig. 7. Plain Image - Knee

and diagnostic data about the patients. To ensure the patient's privacy, it is necessary to safeguard them while they are beingstored and transported.

The traditional cryptographic algorithms such as DES, AES,IDEA, RSA etc., are not suitable for practical image encryp- tion due to computational efficiency and some inherent fea- tures of images such as bulk data capacity, strong correlation among pixels, and high redundancy.
In recent years, chaos has been shown to be a powerful tool in image encryption. Compared with conventional

cryptosys- tems, chaos-based image encryption algorithms have some attractive advantages such as high security, fast speed, rea- sonable computational overheads, and computational power. Chaos-based cryptosystems like Chebyshev polynomials can improve security when paired with conventional public key cryptosystems like RSA and El-Gamal, therefore chaos-based encryption solutions are always preferred for an image orvideo encryption.

Key merits of the chaos-based system:

1. It's an adaptive framework that can resist chosen andknown-plaintext attacks and preserve the security and con- fidentiality of images transmitted through an e-healthcare system.
2. The algorithm produces perfectly uniform histograms formedical images, demonstrating its ability to resist statistical assaults and can be of potential use as a security framework in AI-based healthcare. Apart from histogram analysis, the performance of the scheme is also evaluated for information entropy analysis, statistical analysis, and differential analysis'. 3.Deterministic equations and theorems regulate the be- havior of chaotic systems. Additionally, chaotic systems are designed for protecting the storage and transmission of digitalpictures, coupled with ergodicity and its increased sensitivity to the beginning circumstances.
4. Spatial-domain models include chaotic encryption models.Operations are directly applied to the simple images in spatial-domain models. Many studies integrated spatial and frequencydomain models to increase the security of medical pictureencryption techniques.
5. In order to find the secret keys, one form of chaotic map called a Six-Dimensional Hyperchaotic Map is employed.In comparison to low-order dimensions chaotic maps, it is more dynamic and complex. As a result, guessing the secret keys without knowing the beginning values is challenging. It increases the model's resilience and security.

So, Chaotic cryptography is the application of this theory into cryptographical algorithms to exploit the unique proper- ties of a chaotic system to ensure a more secure encryption system.

VI. FUTURE SCOPE

The future scope of Digital Image Encryption using Hyper-chaotic 6D System and its application in Healthcare is vast and promising. Here are a few potential areas of future research: Improved Security: While Hyperchaotic 6D System is a strong encryption technique, there is always a need to improve

Algorithm	IMAGE 1	IMAGE 2	IMAGE 3	IMAGE 4	IMAGE 5	AVERAGE
Plain Image	7.3578	7.5585	7.1914	6.6777	7.445	-
Proposed	7.99929	7.99926	7.99928	7.99931	7.9993	7.999288
Cosine-transform-based chaotic system	7.999	7.9992	7.9993	7.9992	7.9992	7.99918
Image encryption using 2D Hénon-Sine map and DNA approach.	7.9993	7.9994	7.9992	7.9993	7.9993	7.9993
An image encryption scheme based on chaotic tent map.	7.9921	7.9922	7.9924	7.9926	7.9924	7.99234
Color image encryption based on hybrid hyper-chaotic system and cellular automata.	7.999	7.9991	7.9992	7.9991	7.9995	7.99918
Image encryption using a synchronous permutation-diffusion technique	7.9983	7.9988	7.9991	7.9994	7.9987	7.99886

Fig. 8. Table 1

its security to withstand new and emerging cyber threats. Fu- ture research can focus on developing new and more efficient encryption algorithms that can provide even higher levels of security for medical images.

Integration with Blockchain: The use of blockchain tech- nology in healthcare has gained significant attention in recent years due to its ability to provide secure and decentralized storage of medical records. There is an opportunity to inte- grate Hyperchaotic 6D System with blockchain technology to create a more secure and trustworthy system for storing and transmitting medical images.

Cloud-based Image Encryption: Cloud-based storage and sharing of medical images have become increasingly common.However, this also presents new security challenges. Future research can focus on developing cloud-based image encryp- tion techniques that can protect sensitive medical images fromunauthorized access.

Real-time Image Encryption: In healthcare, real-time trans- mission of medical images is often critical for making timely decisions. Future research can focus on developing real-time image encryption techniques that can provide fast and efficientencryption of medical images without compromising their quality.

Overall, Digital Image Encryption using Hyperchaotic 6D System has tremendous potential for improving the security and privacy of medical images. As technology continues to advance, it is likely that we will see more innovative applications of this technique in the field of healthcare.One such methodology is using Lucas sequence for digital image encryption by generating a random sequence of integers that are used to scramble the

original image data. Lucas sequence encryption achieves secure image encryption by generatinga key stream of pseudo-random numbers using the Lucas sequence. This key stream is then used to scramble the binary data of the original image, making it difficult for unauthorized parties to decode without knowledge of the encryption key.

The following are the main steps involved in using Lucas sequence for image encryption:
Generate Lucas sequence: The Lucas sequence is generated by starting with two specific values, known as the seed values, and then adding them together iteratively to generate subsequent values. This generates a sequence of integers that can be used as a key stream for encryption.
Convert image data to binary: The pixel values of the orig- inal image are first converted to binary form. This is typically done using a fixed number of bits per pixel, depending on the desired level of image quality and encryption security.
Generate encryption key: The Lucas sequence is used to generate a key stream of pseudo-random numbers that are the same length as the binary image data. This key stream is then used as the encryption key to scramble the binary data of the image.
XOR binary data with key stream: The binary data of the image is then XORed with the key stream generated in step 3. This results in a scrambled, randomized form of the original binary data that is difficult to decode without knowledge ofthe encryption key.
Convert binary data back to image: The scrambled binary data is then converted back into pixel values to generate the encrypted image.
Compared to other encryption methods, Lucas sequenceencryption has some advantages. First, it is relatively simple to implement and computationally efficient, as it only involves basic arithmetic operations. This means that it can be imple- mented on devices with limited processing power, such as mobile phones or embedded systems.
Second, Lucas sequence encryption exhibits good statistical properties, such as randomness and uniformity, which are important for cryptographic applications. This means that it can provide a high level of security against attacks, such as brute force attacks or statistical attacks.
However, Lucas sequence encryption also has some limita- tions. For example, it may not provide as strong of securityas other more advanced encryption techniques, such as block ciphers or stream ciphers. It may also be vulnerable to certain types of attacks, such as linear and differential cryptanalysis.

VII. CONCLUSION

The paper proposes a novel technique for image encryp- tion that offers high security and computational efficiency.The technique combines the Fibonacci Q-matrix and the 6D hyperchaotic system to modify the pixel position of an image. The technique also includes double confusion/diffusiontechniques that enhance security. The proposed technique has demonstrated resistance to differential attacks and brute-force attacks, making it a reliable and robust solution for image encryption.

The algorithm's security performance was evaluated using several measures such as information entropy, correlation coef- ficients, noise, data cut attack, and histogram. These measures have shown that the proposed technique offers high levels of security. The secret key used in the technique is also sensitive, adding another layer of security.

The proposed technique can be applied in various fields, including healthcare, where image encryption is crucial toensure the confidentiality and privacy of patient data. Theability to encrypt grayscale images with high-security settings makes the technique an ideal solution for applications where image privacy is paramount.

As encryption technologies continue to evolve, there is a need for a standard benchmark to evaluate the efficiency and efficacy of newly proposed image encryption schemes. The extension of image encryption techniques to video encryption is also an active area of research, suggesting the potential for further advancements in the field.

In conclusion, the proposed technique for image encryption using the Fibonacci Q-matrix and the 6D hyperchaotic system is a robust and reliable solution that offers high levels of security and computational efficiency. Its potential applicationsin various fields, particularly in healthcare, make it a promisingsolution for image encryption.

REFERENCES

[1]. Li, Y.; Yu, H.; Song, B.; Chen, J. Image encryption basedon a single-round dictionary and chaotic sequences in cloud computing. Concurr. Comput. Pract. Exp. 2021, 33, 1.
[2]. Laiphrakpam, D.S.; Khumanthem, M.S. Medical image encryption based on improved ElGamal encryption technique. Optik 2017,

147, 88–102
[3]. Artiles, J.A.; Chaves, D.P.; Pimentel, C. Image encryption using block cipher and chaotic sequences. Signal Process. Image Commun. 2019, 79, 24–31
[4]. OHe, Y.; Zhang, Y.-Q.; Wang, X.-Y. A new image en- cryption algorithm based on two-dimensional spatiotemporal chaotic system. Neural Comput. Appl. 2018, 32, 247–260.
[5]. Zhang, Y. The image encryption algorithm based on chaos and DNA computing. Multimed. Tools Appl. 2018, 77, 21589–21615
[6]. Chai, X.; Gan, Z.; Yuan, K.; Chen, Y.; Liu, X. A novel image encryption scheme based on DNA sequence operations and chaotic systems.
[7]. Xuejing, K.; Zihui, G. A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Process. Image Commun. 2020, 80, 115670
[8]. Zhou, N.; Hu, Y.; Gong, L.; Li, G. Quantum imageencryption scheme with iterative generalized Arnold trans-forms and quantum image cycle shift operations. QuantumInf. Process. 2017, 16, 164.
[9]. Wu, J.; Liao, X.; Yang, B. Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process. 2018, 153, 11–23.
[10]. Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. Nonlinear Dyn. 2017, 87, 127–133
[11]. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt. Lasers Eng. 2017, 90, 225–237
[12]. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. Cyber J. Multidiscip. J.Sci. Technol. J. Sel. Areas Telecommun. JSAT 2011, 1, 31–38
[13]. Yin Daia, Huanzhen Wanga, Zixia Zhouc and Ziyi Jin.Research on medical image encryption intelemedicine sys-tems.Technology and Health Care 24 (2016) S435–S442
[14]. Khalid M.Hosny ,Sara T. Kamal ,Mohamed M. Dar- wish and George A. Papakostas.New Image Encryption Algorithm Using Hyperchaotic System and Fibonacci Q- Matrix.Published: 30 April 2021
[15]. Enayatifar, R.; Abdullah, A.H.; Isnin, I.F.; Altameem, A.; Lee, M. Image encryption using a synchronous permutation- diffusion technique. Opt. Lasers Eng. 2017, 90, 146–154.