IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103058|

Lightweight Medical Image Encryption using Cryptography

R. Sowmiya[1], S. Monisha[2] , S.Monisha[3], S.Madhumitha[4], V. Deepika[5]

Assistant professor, Dept. of CSE, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamilnadu, India[1]

UG Student, Dept. of CSE, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamilnadu, India[2,3,4,5]

ABSTRACT: Medical imaging is of great importance in diagnosis when it comes to the health system. These images contain confidential and sensitive information such as patient xrays, ultrasounds, CT scans, brain images and magnetic r esonance imaging. However, the weak security of the communication channels and the vulnerabilities of the storage sys tems of hospitals or medical centers expose these images tothe risk of being consulted by unauthorized users who exploi t them illegally for nondiagnostic purposes. In addition to improving the security of communication channels and storag e systems, image encryption is a popular strategy to protect medical images from unauthorized access. In this work, we propose a lightweight cryptosystem based on Henon's chaotic maps, Brownian motion and Chen's chaotic systems to en crypt medical images with enhanced security.

The efficiency of the proposed system is measured in histogram analysis, adjacent pixel correlation analysis, contrast an alysis, uniformity analysis, energy analysis, NIST analysis, root mean square error, information entropy, pixel number c hange rate, uniform mean change intensity, peak value, etc. Aspects are demonstrated for noise ratio and expressed time complexity. The experimental results demonstrate that the proposed cryptographic system is a lightweight method that can achieve the level of security required to encrypt confidential patient information based on images.

KEYWORDS: cryptography, medical image encryption, Henon chaos map, Brownian motion, Chen's chaotic system, i mage encryption, Arnold map

I.INTRODUCTION

With the proliferation of smart and smart devices, health records in digital form, and electronic health records more generally, are being generated and continuously distributed online to capture information and achieve accurate results. Electronic health records usually consist of patient information, medical history, symptoms, etc., and are maintained by health care related services. Moreover, in recent years, due to the emergence of COVID-19, many medical images and records have been created online and distributed to medical professionals and healthcare workers. The Bombay High Court denied bail to a man who was on bail for about 10 months in 2021 for falsifying medical documents, while in another case in 2019 IBM reported that the healthcare industry had recorded the most data breaches and that data could be abused in different ways. Additionally, millions of people in the United States were affected by healthcare data breaches in 2015. The initial system conditions are very important because they are keys that only authorized personnel know.Without information about these keys, no one can decrypt the data. In fact, the initial system conditions are sensitive, especially because hackers and unauthorized users often apply minor changes in an attempt to decrypt protected content. The highly sensitive system means that changing tiny values will produce extremely strange calls, so hackers won't be able to decipher the original content. Additionally, the strength of any cryptosystem is judged by its computational complexity, while the transmission rate determines the efficiency of the overall system.

II.SYSTEM MODEL AND ASSUMPTIONS

HENON CHAOTIC MAP

The Henon chaotic map (HCM), sometimes termed a Henon–Pomeau attractor map, is a dynamic system of the discrete domain and one of the most reviewed examples of two-dimensional dynamic structures that exhibit unpredictable/chaotic behaviours. The Henon map functions by taking any point along the plane (x_n , y_n) and mapping it to a new one, a process that can be formulated as follows:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103058|

$$x_n + 1 = 1 - ax_n^2 + y_n$$

$$y_n + 1 = bx_n$$

As shown above, this chaotic map depends on parameters a and b. Additionally, the system was built to set values of a = 1.4 and b = 0.3. The Henon map is chaotic with respect to conventional values, but may appear chaotic, jerky, or converge to an aperiodic orbit for other values of the same parameter.
Insight into the behavior and shape of Henon's map at different values
of its parameters can be obtained from its orbital plot. 2D chaos diagram plotted for 10,000 iterations with initial conditi ons set to a = 1.4 and b = 0.3

BROWNIAN MOTION

Brownian motion is the spontaneous motion of particles floating in a liquid or gas and is the result of interactions betwe en fast moving atoms and molecules. The evolution of a particle along three main directions (here X, Y and Z), defined mathematically by

$$x= \ rsinacosb \ , y=rsinasinb \ , \ z=rcosa$$
$$and \ 0 \leq r \leq +\infty, 0 \leq b \approx, \ 2 \ 0 \leq a \leq \pi$$

The state of a Brownian particle can be measured when there is enough information about the direction of motion of the particle, i.e. the motion of the particle in three directions (X Y Z). The specific duration (tp) is the time required for the particle to move irregularly, the total number of particles involved in the zigzag motion (np), and the number of pulses per change of orbit associated with the smooth zigzag motion.
The step size is denoted r = 2, and a pseudo-
random function is used to determine the direction of particle motion. In this way, the X, Y and Z characteristics of each Brownian particle position can be obtained. BM can be generated using a Monte Carlo process. In the 3D model, 2D chaotic maps, initial conditions a=1.4, b=0, iteration 1000 times.
3 We estimate the Brownian motion of 10 particles using a 10×3 vector to store the Brownian momentum of the particle s for each change in trajectory, particle position and distance. Plots in all three directions. The proposed scheme is for th e number of particles (np) = 256, the total estimation time (t) = 60 s and the number of pulses per trajectory change = N = 100 × t (where: t = 60 s).

CHAOTIC CHEN SYSTEM

The chaotic system based on is defined as follows:

$$\frac{dx}{dtdy} = a(y - x) => dtdz$$
$$(c - a)x - xz + cy$$
$$xy - bzdt$$

Here a, b, and $c \in R^3$ are fixed.

If a=35,b=3 , and c=35 . then the system involves a chaotic attractor

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103058|

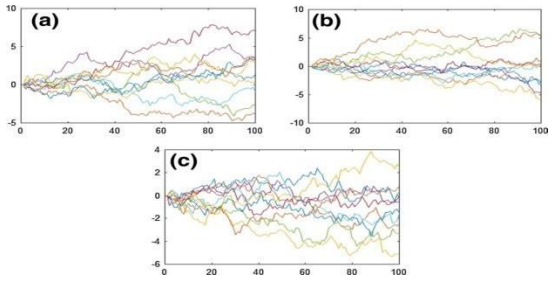
The fractional order of this particular system may be defined as:

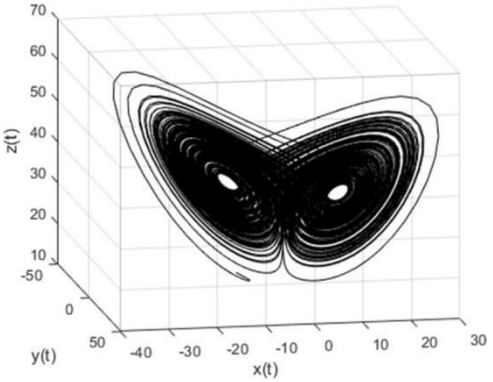
$$\frac{dxqdy}{dz} = (c-a)x - xz + cy$$

$$=> \quad xy - bzdt_q$$

$$=> \quad dt$$

Where$q$ reflects a fractional order with a specific range of $0<q<1$. Therefore, we change only the derivative order q and the system parameter c in this simulation process while





3D view of a CCM attractor in a fractional Chen system of particle

s with Brownian motion

along the X (a), Y (b) and Z (c) directions for np=10, t=10 s and N/T

=10 (4) q= 0.1 while (a, b, c) = (35.3 3, 28)

The remaining input variables remain unchanged. Note that q and c are changed. Perform the simulation with a step size of 0.1 and q = 0.

6–0.1. Here, the simulation results show that when the order exceeds 3, chaos tends to exist. And q = 0.6–0.

1 At time step 0.1, there is also a chaotic attractor, as shown in Figure 1. As shown in Figure 6, this demonstrates. Howe

ver, for a value of q = 0, no chaotic behavior is observed, implying that q = 0-

0.1 is the lowest fractional q limit at which chaos can exist in such systems (4)

0.3 is the lowest order we can distinguish from chaos

III.FUNCTIONALITIES

HISTOGRAM ANALYSIS

The proposed scheme is tested on various gray medical images, including chest, brain, and MR, and the results are displ ayed. In the first step of the proposed scheme, the pixels are swapped (mixed) to get the output. Each medical image is encrypted along three directions, the pixels of the histogram of each medical image are not uniformly distributed in thes e three directions, but each pixel of the encrypted image is uniformly distributed along three different directions.

ADJACENT PIXELS CORRELATION ANALYSIS

The correlation coefficient ranges from 1 to 1, where 1 indicates exact similarity between two images or pixels. For the case of maximally irrelevant pixels, i.e. highly random values, values close to 0 should be obtained. The pixel-level similarity or dissimilarity between plaintext and ciphertext of different medical images is investigated

HOMOGENEITY, ENERGY AND CONTRAST ANALYSES

Contrast is the difference in brightness or color by which elements of an image can be distinguished and viewers can ide ntify different objects. The difference in intensity of adjacent pixels throughout the image can be calculated by contrast analysis. For added security, the contrast value should be higher to reveal the randomness of the cipher text image.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103058|

NUMBER OF PIXELS CHANGING RATE

The number of changing pixels in two cipher text images can be calculated via the NPCR test when there is a minute difference of one pixel between their plaintext images

PIXEL'S INCONSISTENCY ANALYSIS

For any robust cryptosystem, the measure of MSE must be high. We apply the MSE test to the three medical images in t hree different orientations. Mean MSE values
(across all orientations) were 11017, 12320, and 11468 for chest images, brain images, and MRI images, respectively. T he evaluation values
of the proposed scheme are also compared. The higher value obtained by our proposed scheme shows that it is very sec ure even compared to the most modern cryptosystems

TIME COMPLEXITY

An efficient cryptosystem should consume minimal resources and time when running. Analysis time and computational complexity requirements

VI.CONCLUSION

In this paper, we spotlight the encryption for security purposes of the medical images. The proposed system of this paper implies the secure transmission of online medical images

REFERENCES

[1] https://file.techscience.com/ueditor/files/cmc/TSP_CMC-73-1/TSP_CMC_28789/TSP_CMC_28789.pdf
[2] https://www.researchgate.net/publication/349599982_Lightweight_Encryption_Technique_to_Enhance_Medical_Image_Security_on_Internet_of_Medical_Things_Applications
[3] https://link.springer.com/article/10.1007/s11277-021-08584-z
[4] https://www.sciencedirect.com/science/article/pii/S187705091502181X

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details