A NOVEL APPROACH FOR CLOUD-BASED MEDICAL DATA ENCRYPTION USING HENON CHAOTIC MAP

Uma Hombal[1] and Dayananda R. B.[2]
Department of Computer Science and Engineering

[1]Research Scholar, KSIT, Bengaluru, [2]Associate Professor, MSRIT, Bengaluru

ABSTRACT

The ability to send enormous files was made possible by recent developments in networking technologies that increased network bandwidth. Multimedia data, in particular digital images, makes up a sizable amount of the files being sent across various networks worldwide. In this research, we suggest a brand-new encryption method that might be applied to protect data (text and medical image). The cypher image is produced using the technique using a 128-bit secret key and the Henon chaotic map. The Henon chaotic map is a discrete, iterative, two-dimensional dynamic system that exhibits chaos depending on the values of the input constants. Chaotic maps are extremely sensitive to the starting parameters; hence, even a small change in the early circumstances has a significant impact on the chaotic system's overall output. In our approach, the original image is encrypted using the Henon chaotic map and a 128-bit secret key that is supplied externally. A permutation matrix created using the chaotic map is used to execute pixel shuffle after the image has been encrypted. A standard collection of lab data is used to verify the algorithm's performance using metrics including peak signal to noise ratio (psnr), NPCR, UACI, and MSE.

KEYWORDS

Image Encryption, Henon Chaotic Map, Fully Homomorphic Encryption, NPCR, UACI.

1. INTRODUCTION

The ideal way to retain the patient's records is through an electronic health record, which will help the quality of healthcare. A digital record of a patient's medical information is called an EHR. This technology has a number of benefits over using paper records. Maintaining a huge number of records is made easier with the use of electronic health records, which also make it simple to enhance patient care in all respects, including efficiency and accurate, instantaneous record updates. The patient health management features in this medical record system also contain listings of medications, diagnostic tests, physical examinations, previous history observations, and laboratory findings. Multiple people can each access the same patient record. These records are kept on a public cloud.

Ensuring the security of image information is vital for the overall security of network systems. This is intricately connected to individuals' daily lives and has a direct impact on their personal reputation and the security of their assets. The demand for robust image information security has become pressing, largely driven by the extensive integration of high-speed Internet technology. As a result, the security of image information has been examined by a large number of mathematicians, cryptologists, chaotic scientists, and image processing professionals [1] [2] [3] [4]. As a result, several good image cryptosystems have been developed, considerably accelerating the development of this research subject.

The Internet, a widely used public network, is used today to send enormous amounts of information (in the form of text, images, music, or video) around the globe. Although effective, the Internet is quite unsecure and as a result is vulnerable to numerous dangers [5][26]. The significance of safeguarding sensitive images is paramount to thwart unauthorized access by external entities. The security of images relies heavily on cryptography, a universally acknowledged approach for ensuring information and image protection. Cryptography involves the conversion of data into an incomprehensible and indecipherable format through encryption, guaranteeing that solely authorized individuals possess the

means to restore the information through decryption processes. [6] [7].

Many encryption techniques simply use a one-dimensional or two-dimensional chaotic environment in order to boost their efficiency [8-11]. The predictability of chaotic systems enables attackers to potentially deduce the corresponding chaotic orbit information. With this information at hand, attackers could leverage existing analytical techniques to identify the structural characteristics of the chaotic system, thereby reducing the complexity of deciphering the encryption key. [12].

The homomorphic encryption approach improves the security features of untrusted systems or applications. It converts the information into cipher text, which is deconstructed and worked with as if it were still in its original form [4]. It allows for the processing of intricate mathematical operations on encrypted data. As a result, the encryption process is a secure system in which security is not compromised.

A cutting-edge field called chaos based cryptography uses multiple chaotic maps to create random sequencing for the encryption of digital medical images [24]. The inherent traits of these simple chaotic maps include nonlinearity (NL), responsiveness to initial conditions, presence of unique attractors for different initial keys, and elements of randomness. These particular attributes have the potential to form the foundation of a robust cryptographic system.

2. LITERATURE SURVEY

Numerous approaches are commonly employed to ensure the confidentiality of data stored in cloud environments. One prevalent strategy in managing digital patient healthcare information is through electronic health records, particularly favoured due to the immense data volume involved. The central concern in cloud computing remains security, prompting the availability of diverse cryptographic algorithms designed to safeguard cloud-based data. To facilitate the secure transmission of encrypted electronic hospital records, a lightweight encryption method is recommended. For delivering encrypted data, the TSFS technique is proposed, accompanied by the execution of picture segmentation. The integration of Hadoop and MapReduce is employed for image compression. As a result of this approach, the privacy of medical data can be reliably upheld. [14].

Sharing of private images must be done with caution. This cannot be done without revealing the original image, and only an effective public key cryptosystem can. The homomorphic property is used to transmit the hidden pictures. Both the multiplicative and additive homomorphic properties are satisfied by RSA and Pascalier, respectively. The image is encoded using these two techniques. When choosing the size of the pixel block, the RSA technique must be used with caution. This technique lowers the cost of calculation and is applicable to many applications [15].

Since the user no longer controls the image, the suggested encryption scheme is used on cloud storage [16]. Because the server doesn't know the secret keys, the authors must encrypt the image. Hyper Chaos map implements the hidden keys in this algorithm. The confusion-diffusion architecture of the suggested technique was designed using several XOR operations in the proposed encryption algorithm. Both colour and grayscale photos can use this technique.

Medical photos that can be transformed using cloud computing are used to test the suggested encryption technique [17]. This algorithm shields sensitive images from servers and unauthorized users while they are being transformed. They made advantage of the chaotic key generator map. This scheme's confusion process is designed by secret keys and the XOR mathematical operation, which makes the algorithm secure.

In this approach [18], the image is encrypted using an improved logistic map, block scrambling, and zigzag transformation. The image was blurred using a permutation and diffusion procedure. The modified logistic map is used in this technique to create secret keys, making it secure. The confusion-diffusion architecture of the image is implemented by this scheme's use of the pixel shuffle technique.

In this technique, they proposed image compression in cloud storage using symmetric key homomorphism cryptography [19]. They increase the suggested scheme's security system by using

stenography and contrast augmentation. This algorithm makes use of reversible data concealment. Both color and grayscale images can use this pattern.

They suggested an innovative cloud-based image encryption technique [20]. They use the two-dimensional Fractional Fourier Transform and the two-dimensional Discrete Fourier Transform in this approach to encrypt the image. The process of encoding and decoding images uses a random phase matrix. These two procedures put this system's confusion-diffusion architecture into practice.

3. PROPOSED METHODOLOGY

3.1 Henon Chaotic Map (HCM):

Because chaotic maps are so sensitive to the starting conditions, cryptographic techniques frequently employ them. Chaotic maps are used in a number of picture encryption methods. The following phases make up a chaotic technique's general approach:

i. During the "pixel shuffling" or confusion phase, pixel rearrangement occurs, leading to the disentanglement of pixel relationships. Following this step, essential statistical aspects such as the image's histogram remain unaltered.
ii. Changes to pixel values are made during the diffusion phase of pixel modification.

The three classes of chaotic methods are derived from the methods mentioned above: methodologies involving pixel permutation or transposition, techniques that solely alter pixel values, and visual transformation methods that amalgamate both pixel modification and transposition procedures. One of the extensively examined cases of two-dimensional dynamic structures exhibiting unpredictable or chaotic characteristics is the Henon chaotic map (HCM), alternatively recognized as a Henon-Pomeau attractor map [25]. It constitutes a dynamic system within the discrete domain.

Any location along the plane serves as the starting point for the Henon map (x_n,y_n) with a new one being mapped to it. It can be described as the following process:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (1)$$

In terms of conventional values, a Henon map is chaotic, but for various values of the same parameters, it may turn out to be chaotic, intermittent, or else converge to an aperiodic orbit. The Henon map's orbit diagram summarizes its behavior and shape for various values of its parameters

3.2 Fully Homomorphic Encryption (FHE):

If two operations, namely addition and multiplication, may be performed on encrypted data an infinite number of times, then the encryption method is fully homomorphic. In all fully homomorphic encryption methods, ciphertext contains noise that gets louder as operations progress. Particularly, when compared to addition, a multiplication action produces greater noise. At a certain point, the noise level becomes too high, prohibiting additional homomorphic processes from yielding accurate results. The performance is now seriously lacking because a refreshing operation is necessary.

Patient health records are known as Electronic health records (EHR) in the healthcare sector. Hospitals or other healthcare facilities maintain these digital records of patient's medical histories. It contains demographic information, medical records, medical histories, and clinical data. Electronic health records (EHRs) are formal recordings of medical data produced by any healthcare professional. The quality of service and cost-effectiveness are projected to increase with the digitization of patient health information. Additionally, it makes it feasible for patients' medical records to be accessed whenever and wherever they are needed. The major objective of EHRs is to bridge the communication gap between healthcare professionals in order to deliver better care at lower costs.

Homomorphic addition of two numbers: The sum of two ciphertexts corresponding original numbers will be revealed if we take the product of the two.

Dec (Enc (A,r1).Enc (B,r2) mod n^2) = (A+B) mod n, where A and B are real numbers

4. SIMULATION AND ANALYSIS

Only after carrying out certain test analysis is it possible to determine how effective an image encryption procedure is. The following analyses are carried out in this research.

i. Key Space Analysis:

The secret key in this work is 150 bits long, and the key space is about 2^{150}. The brute force approach is difficult to use against an encrypted image with a key size of 2^{150}. As a result, the size of this key is adequate.

ii. Histogram Analysis:

Histogram analysis can be used to determine how an image's pixels are distributed. This security study provides the statistical characteristics of the encrypted image. A histogram with a constant distribution characterizes a perfect encrypted image. As a result of this study, we can create a graph with randomly dispersed streaks. By analyzing this graph, it becomes possible to assess whether the applied algorithm effectively encrypts the entire image or if any part of the image remains inadequately encrypted. A series of images, paired with their respective encrypted versions, were captured for the purpose of this study. Figure 1 illustrates the histogram of the original image. An observation was made regarding the uneven pixel distribution. The histogram of the encrypted image is also presented, demonstrating a consistent pixel distribution. The uniformity in the encrypted image's histogram poses a challenge in discerning the statistical pixel composition of the original image. Through this histogram analysis, it has been established that a sound cipher image generates a histogram with a uniform pattern. [23].

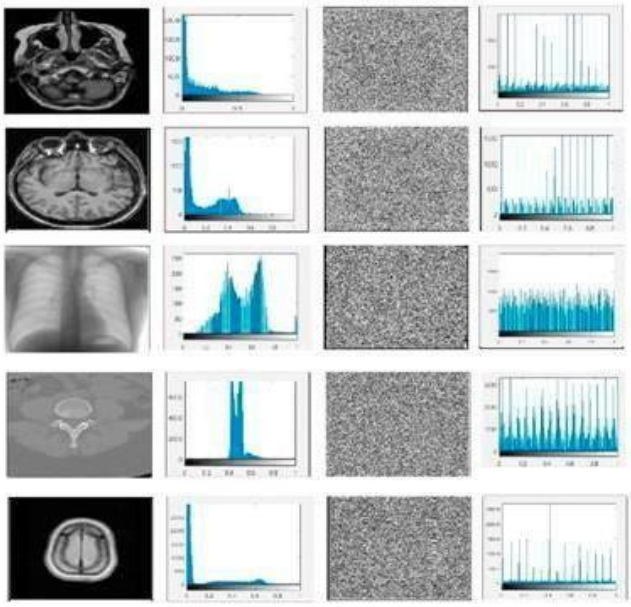


Figure 1. Histogram of original and unencrypted medical images.

iii. NPCR and UACI Definitions:

As far as we are aware, Yaobin Mao and Guanrong Chen are the subjects of both NPCR and UACI, which were first published in 2004 [21, 22]. Since then, NPCR and UACI have grown to be two of the most popular security analyses for differential threats in the image encryption sector.

Suppose the ciphertext images prior to and after a pixel change in a plaintext image are C^1 and C^2 respectively; the grid's pixel value (i,j) in C^1 and C^2 are denoted as $C^1(i,j)$ and $C^2(i,j)$;

and a bipolar array D is defined in equation (1). The NPCR and UACI can then be formally described using Equations (2) and (3), respectively, where symbol T indicates how many pixels there are in the ciphertext overall, symbol F shows the largest number of pixels that can be used with the ciphertext image format and |.| represents the absolute value function.

$$D(i,j) = \begin{cases} 0, if\ C^1(i,j) = C^2(i,j) \\ 1, if\ C^1(i,j) \neq C^2(i,j) \end{cases} \quad (2)$$

$$NPCR: \mathcal{N}(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \quad (3)$$

$$UACI: \mathcal{U}(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F.T} \times 100\% \quad (4)$$

The NPCR metric distinctly emphasizes the precise quantity of altered pixels during differential attacks, whereas UACI centers around the mean difference between two corresponding pairs of ciphertext images. The range of NPCR lies within [0, 1]. An NPCR value of 0 signifies that all pixels in C^2 possess identical values as those in C^1 . Conversely, an NPCR value of 1 indicates that each pixel value in C^2has undergone modification compared to C^1 . Establishing associations between these two ciphertext images, C^1 and C^2, proves to be exceedingly intricate. The occurrence of N(C^1 , C^2) = 1 is rare, primarily due to the fact that even two independently generated truly random images seldom consistently attain the maximum NPCR, particularly when dealing with relatively larger image sizes.

Similarly, the UACI range is confined within [0, 1]. However, determining the optimal UACI value for two encrypted images remains less evident. Fortunately, the subsequent sections will provide the necessary insights into these values, including expectations and variances.

The application of NPCR and UACI assessments is common in evaluating the cipher's resilience against differential attacks in image encryption. These tests are particularly useful when dealing with minor deviations between plaintext images, often involving just a single pixel alteration. NPCR examines the count of altered pixels, while UACI calculates the average intensity change between corresponding ciphertext images. Despite their straightforward definitions and ease of calculation, deriving sufficient performance conclusions from test outcomes can be a challenging endeavor.

iv. MSE and PSNR Analysis:

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are calculated for the benchmark images.

$$MSE = \frac{1}{N*M} \Sigma_{n=1}^{N} \Sigma_{m=1}^{M} [|f(i,j) - f_0(i,j)|^2] \quad (5)$$

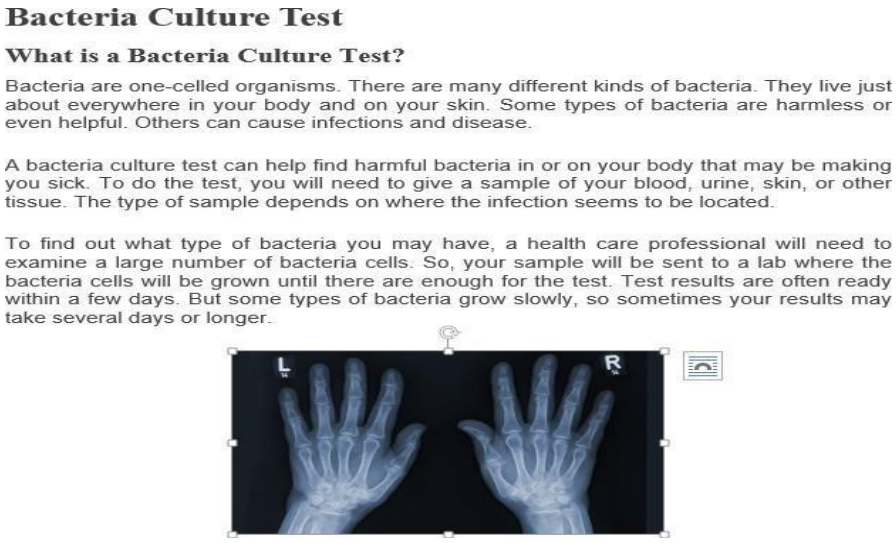
The Peak Signal-to-Noise Ratio (PSNR) represents the relationship between the maximum mean square difference observed between two images and the mean square difference inherent to those images. Enhanced image quality is indicated by higher PSNR values.

$$PSNR = 20 * log \frac{255^2}{\sqrt{MSE}} \quad (6)$$

v. Performance Analysis:

Comparison is carried out between chaotic mapping and Homomorphic based on MSE, PSNR, UACI and NPCR parameter. It is found that HCM resulted better in comparison with Homomorphic Encryption.

Sample Lab text information and image of a patient considered for demonstration of performance analysis.



Bacteria Culture Test

What is a Bacteria Culture Test?

Bacteria are one-celled organisms. There are many different kinds of bacteria. They live just about everywhere in your body and on your skin. Some types of bacteria are harmless or even helpful. Others can cause infections and disease.

A bacteria culture test can help find harmful bacteria in or on your body that may be making you sick. To do the test, you will need to give a sample of your blood, urine, skin, or other tissue. The type of sample depends on where the infection seems to be located.

To find out what type of bacteria you may have, a health care professional will need to examine a large number of bacteria cells. So, your sample will be sent to a lab where the bacteria cells will be grown until there are enough for the test. Test results are often ready within a few days. But some types of bacteria grow slowly, so sometimes your results may take several days or longer.

Figure 2. Sample lab record

Table 1. Chaotic Mapping Performance Analysis

Test Cases	MSE	PSNR	UACI	NPCR
Lab1	11436.34	7.55	34.17	99.61

Table 2. Homomorphic Performance Analysis

Test Cases	MSE	PSNR	UACI	NPCR
Lab2	18101.49	5.55	43.65	99.14

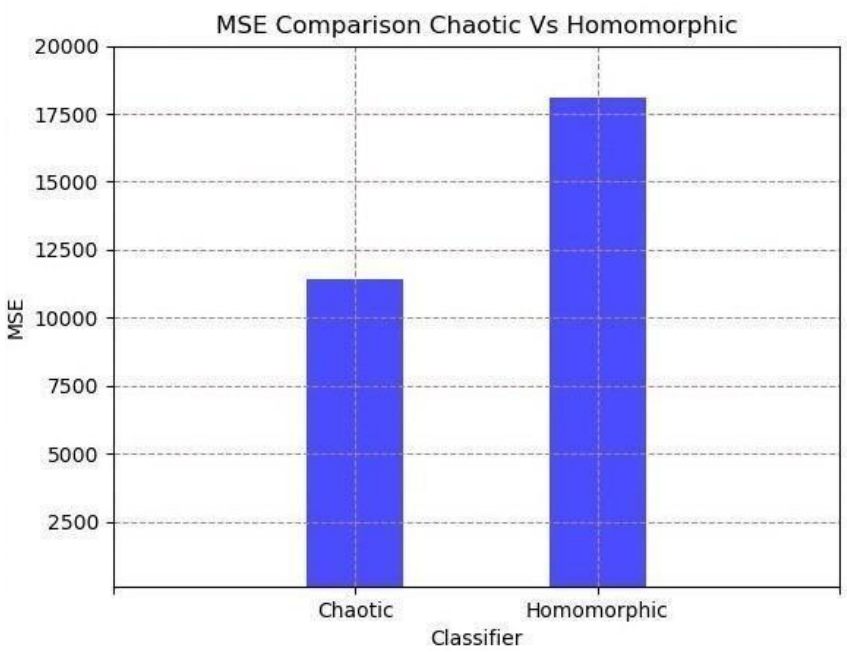


Figure 3. Comparison based on MSE.

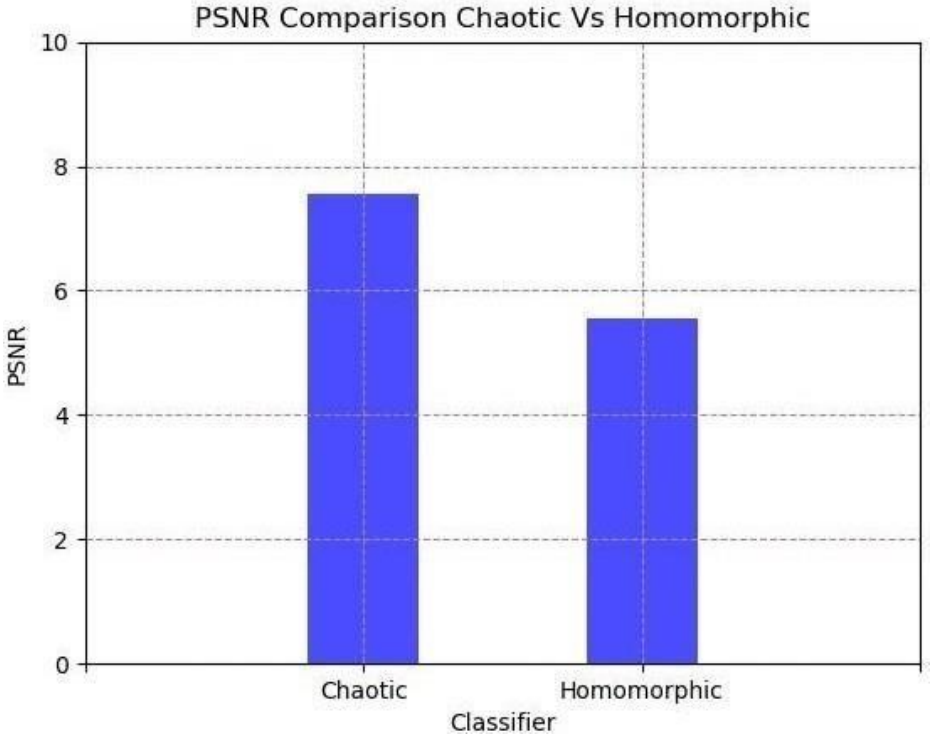


Figure 4. Comparison based on PSNR

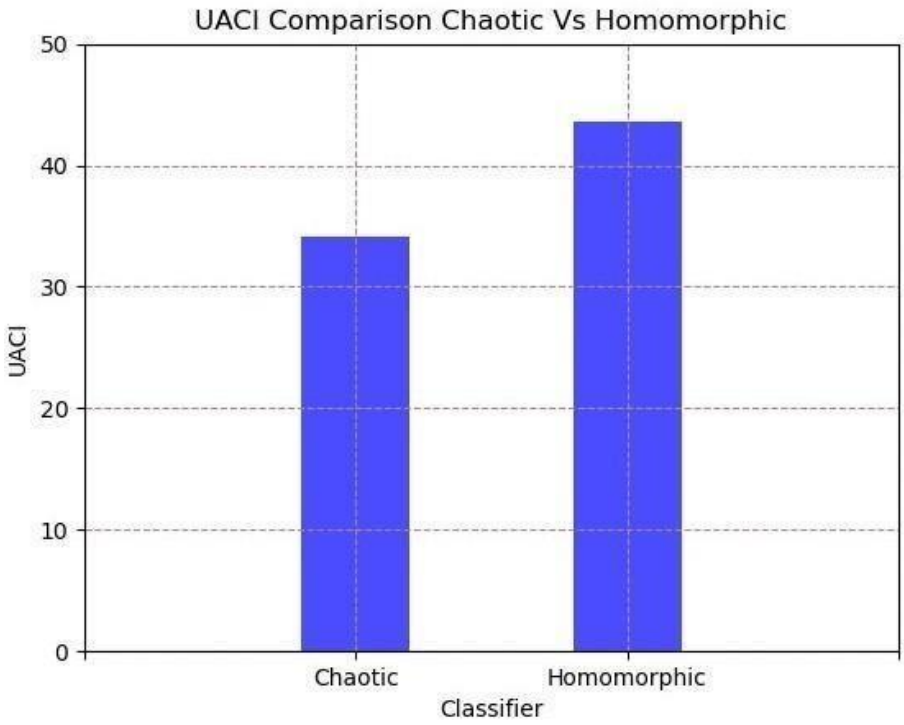


Figure 4. Comparison based on UACI

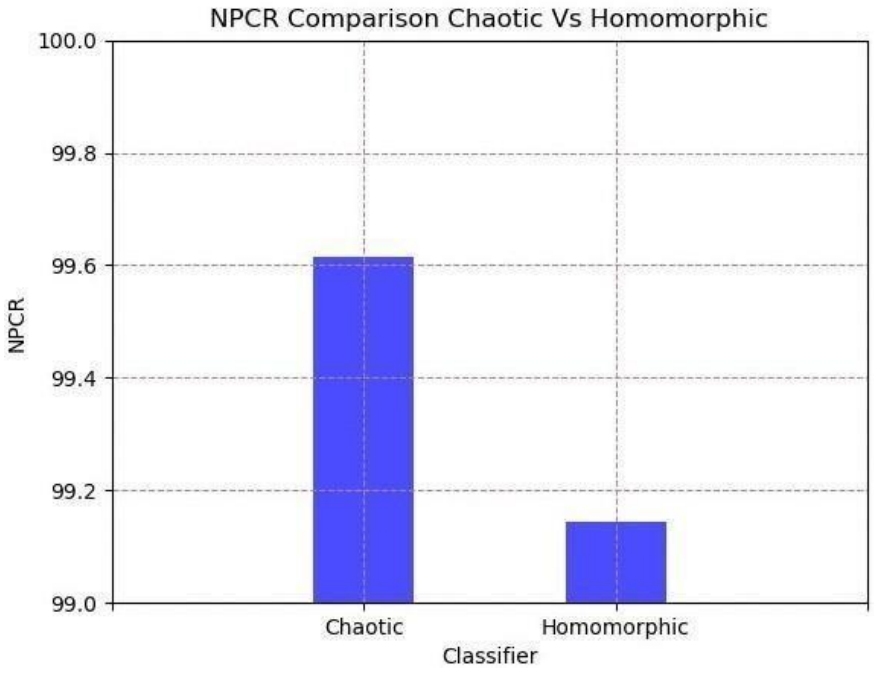


Figure 5. Comparison based on NPCR

5. CONCLUSION

This paper introduces an innovative image encryption approach. The approach capitalizes on the chaotic properties of the Henon map functioning as a pseudo-random number generator. Coupled with a confidential 128-bit key, this method generates a permutation matrix for reordering the original image. Subsequently, a cipher image is employed to encrypt the reorganized image. Comprehensive evaluation of this technique is conducted, involving benchmark test images and adherence to diverse security standards for digital image encryption. Based on performance analysis carried out between Henon Chaotic Map and Fully Homomorphic Encryption, it is found that for various testing

parameters, HCM has outperformed better accuracy for providing security over cloud with respect to text information and image of a patient.

ACKNOWLEDGEMENTS

The authors would like to thank Dept. of CSE of MSRIT and Dept of CSE of KSIT for their support and encouragement !

REFERENCES

[1] X. Chai, Z. Gan, K. Yuan K, Y. Chen, X. Liu, A novel image encryption scheme based on DNA sequence operations and chaotic systems, Neural Computing and Applications 31 (1) (2019) 219–237.

[2] J A. Gutub, M. Al-Ghamdi, Hiding shares by multimedia image steganography for optimized counting-based secret sharing, Multimedia Tools and Applications 79 (2020) 7951-7985.

[3] A. Gutub, N. Al-Juaid, E. Khan, Counting-based sharing technique for multimedia applications, Multimedia Tools and Applications 78 (2019) 5591-5619.

[4] Z. Hua, Y. Zhou, Image encryption using 2D Logistic-adjusted-Sine map, Information Sciences 339 (2016) 237–253.

[5] Abd El-Samie, E. F., Ahmed, H. E. H., Elashry, F. I, Shahieen, H. M., Faragallah, S.O., El-Rabaie, M. E., and Alshebeili, A. S., Image Encryption- A Communication Perspective. 1st Ed., CRC Press, London, (2014), pp.: 1-86.

[6] Mishkovski, I. and Kocarev, L., Chaos-Based Public-key Cryptography, Springer-Verlag Berlin Heidelberg, SCI 354, (2011), pp.: 27-65.

[7] Abraham, L., and Daniel, N., "Secure Image Encryption Algorithms: A Review", International Journal of Scientific and Technology Research, Vol. 2, No. 4, (2013), pp.: 186 – 189.

[8] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," Multimedia Tools and Applications, vol. 78, no. 9, pp. 12027–12042, 2018.

[9] L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, "A novel image encryption scheme based on nonuniform sampling in block compressive sensing," IEEE Access, vol. 7, pp. 22161–22174, 2019.

[10] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics Communications, vol. 284, no. 12, pp. 2775–2780, 2011.

[11] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," Signal Processing, vol. 143, pp. 122–133, 2018.

[12] Y. P. Zhang, F. Zuo, and Z. J. Qu, "A survey of digital image encryption based on Chaos," Computer Engineering & Design, vol. 32, no. 2, pp. 463–466, 2011, (In Chinese).

[13] 'A New Hybrid Homomorphic encryption scheme for cloud data security', ACST Vol 10, ISSN 0973-6107, April 2017.

[14] Jitender Madarkar, Anuradha D, Sachendra Waghmare .Security Issues of Patient Health Records in E-hospital Management in cloud International Journal of Emerging Research in Management and technology; 3 (6): 46-51.

[15] Naveen Islam, William Puech, Khizar Hayat, Robert Brouzet. Application of Homomorphism to Secure Image Sharing. Elsevier 2011; 284 4412-4429.

[16] S. Ayyub and P. Kaushik, "Secure Searchable Image Encryption in Cloud Using Hyper Chaos", the International Arab Journal of Information Technology, Vol. 16, pp. 2, 2019.

[17] S. Kurnaz and A. A. Jasim, "Cloud System for Encryption and Authentication Medical Images", IOSR Journal of Computer Engineering, Vol. 20, pp. 65-75, 2018.

[18] P. Ramasamy, V. Ranganathan, S. Kadry, R Damasevicius,and T. Blazauskas, "An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map" , Entropy, Vol. 21, pp. 656, 2019.

[19] G. Preethi and N. P. Gopalan, "Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage", International Journal of Applied Engineering Research, Vol. 6, pp. 3861-3866, 2018.

[20] S. Altowaijri, M. Ayari and Y. El. Touati, “A Novel Image Encryption Approach for Cloud Computing Applications”, International Journal of Advanced Computer Science and Applications, Vol. 9, pp. 12, 2018.

[21] G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons and Fractals, vol. 21, pp. 749-761, 2004.

[22] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps," Int. J. Bifurcation and Chaos in June, 2003.

[23] C. Samson, V. Sastry. A novel image encryption supported by compression using multilevel wavelet transform. Int. J. Adv. Computer. Sci. Applied 2012; 3 (9): 178–183.

[24] Wang, X., Wang, Y., Zhu, X., & Luo, C. (2020b). A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. Optics and Lasers in Engineering, 125, 105851.

[25] Henon, M. (1976). A two-dimensional mapping with a strange attractor. In The theory of chaotic attractors (pp. 94–102). Springer.

[26] U. Hombal and R. B. Dayananda, "A Review on Security and Privacy Preserving Mechanisms of Electronic Health Records in Cloud," 2021 Asian Conference on Innovation in Technology (ASIANCON), PUNE, India, 2021, pp. 1-4, doi: 10.1109/ASIANCON51346.2021.9544547.