Two-Fold Cryptography: Enhancing Image Security with Henon Map

Saad A. Abdulameer[1]

[1]*Computer Department, College of Education for Women, University of Baghdad*

[*]*Corresponding Author:* saad@coeduw.uobaghdad.edu.iq

Received 1 Oct. 2024, Accepted 4 Dec. 2024, published 30 Dec. 2024.

DOI: 10.52113/2/11.02.2024/140-154

Abstract: This paper introduces an innovative method for image encryption called "Two-Fold Cryptography," which leverages the Henon map in a dual-layer encryption framework. By applying two distinct encryption processes, this approach offers enhanced security for images. Key parameters generated by the Henon map dynamically shape both stages of encryption, creating a sophisticated and robust security system. The findings reveal that Two-Fold Cryptography provides a notable improvement in image protection, outperforming traditional single-layer encryption techniques.

***Keywords*:** chaotic map, Henon, image encryption, cryptography, security

1. Introduction

The increasing importance of the multimedia information exchange, owing to further development of communication technologies, has given rise to the issue of image security. Data security is best achieved when the images need to be protected, thus demand for efficient encryption techniques necessitates the need to continue to come up with new and efficient one. In addition, increased incorporation of artificial intelligent in designing of secure systems has greatly contributed to improving, especially, the security standards [1].

Cryptography generally follows two main approaches: It deals with two types of encryption: a symmetric encryption system in which the two parties use the same key for encrypting and decrypting; and a public-key encryption system in which information is encrypted by one's public key and decrypted with a recipient's private key. It was showed that, both approaches are useful where there is an increasing concern with the security of data [2].

Presently there is a transfer and storage of humongous data through electronic media as the world shifts to digital conventional data security becomes a core issue. In the last decades encryption has emerged as a need for protection of data as it traverses untrusted networks such as the Internet. As time passed on and technology improved, encryption has become more paramount in protecting data that is stored or processed based on the cloud systems [3].

Many encryption algorithms have been created to enhance the privacy and confidentiality of any secured data. Of the above, it can be stated that encryption methods based on chaotic maps with dynamic keys reveal the highest effectiveness and demonstrate a multitude of potential prospects for further enhancement. These techniques have been successfully used in encrypting text, voice, image, and video [4]. Apart from the usual programs like AES, IDEA, and DES, there are improved types of cryptography to improve the cryptographic image for digital image. These methods usually incorporate a confusion-diffusion framework, where the pixel positions are rearranged, and pixel values are altered—see Figure (1) for how the images are secured.

This has led to the emergence of what is today referred to as image security due to need to protect information from forgery and loss. The Henon chaotic system has been proved to be competent and innovative through the newly developed symmetric encryption algorithm that ingeniously employs the byte sequences for pixel complex displacement, in order to increase image security.

Therefore, image encryption is relevant to ensure protection of data when transmitted through insecure channels it is therefore important to ensure protection of data when transmitted through insecure channels. As technology and associated communication channels continue to develop, secure mathematical techniques have emerged as critical for preserving confidentiality of data [5].

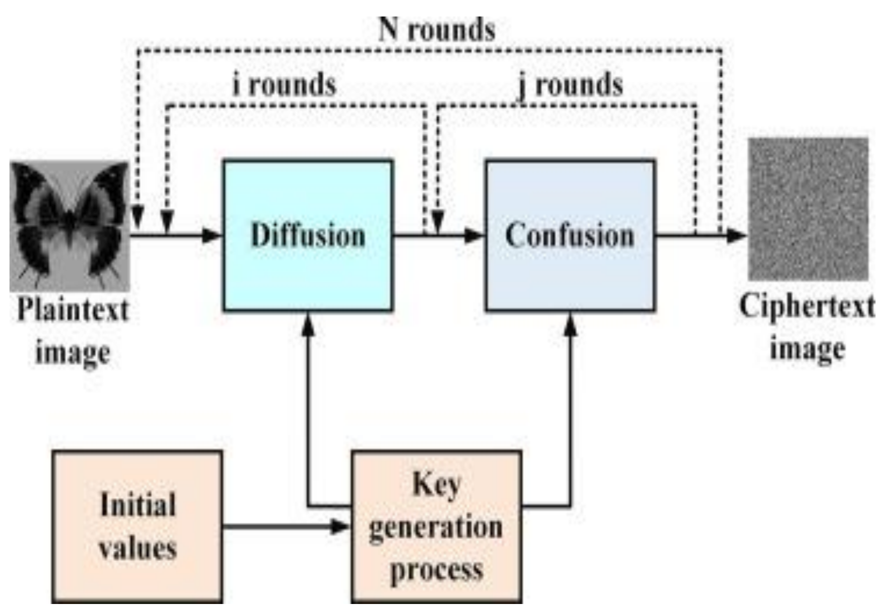

Fig. (1): A classical image encryption process [3].

2. Methodology

2.1. Background on image encryption

The later challenges have emerged in light of the growing rapidly use of digital images making it important to enhance their security in the present days. Since images are often uploaded and saved in multiple digital interfaces their protection from unauthorized access and alteration requires utmost attention. Nevertheless, AES and DES encryption techniques pose challenges in the complete protection of images, which has readily revealed the need for more enhanced and secured approaches.

Recently, security of the image encryption algorithms has enhanced by the use of a new technique called chaotic cryptography. Its attractiveness is based on natural pseudo-randomness and certain randomness which characterize chaotic systems. These systems further improve encryption by displacing and distorting the image pixel arrangement using the Hénon map and Arnolds cat map [7].

The benefits of using chaotic systems in image encryption includes; high speed, high security, and complexity of the method and efficiency. These characteristics make chaotic-based encryption a reasonable solution to overcome the drawbacks of traditional ciphers in protecting digital images [8].

Modern advances in image encryption have raised new approaches that facilitate the manner in which images are confused and spread through spatiotemporal chaotic systems. Furthermore, bit-level displacement algorithms are employed to modify the pixel intensity and enhance the encryption benefits [9].

In general, chaotic-based encryption methods synthesize a sufficient security for a digital image, while they are transmitted and stored, thus reaching the need for explicitly secure methods in the modern world [10].

2.2. Overview of two-fold cryptography

In the exponentially increasing technological advancement, especially, in the field of digital technology the necessity of possessing measure data security becomes essential especially when it comes to military operations, health care delivery, and conducting of business both online and offline transactions. In these fields, fast and reliable security for data transmission is needed. A lot of information and redundant data and repeated information make image encryption much more complex than AES or DES. Chaotic theory based encryption techniques seems to be more promising when compared to traditional encryption techniques which has many advantages such as high speed of encryption, highly complex and optimized in terms of computational resources.

In general, Chaotic maps share some characteristics that apply well to the process of image encryption, these are; unpredictability, sensitivity to initial conditions and most importantly the randomness. These characteristics have particularly an important function during confusion and diffusion processes in the encryption. It has been established that there are many encrypting techniques that have been proposed using chaotic maps [11] to demonstrate how chaotic theory can enhance image security remarkably. Out of them which is quite noteworthy is known as Henon map which is applied to improve image security. The Henon map displays a chaotic attribute, and this paper utilizes it for developing an encryption sequence to shuffle the pixels and use bitwise XOR techniques in the encryption scheme. It has a two-layered structure: applying chaotic maps [8] makes this method more secure in comparison with the first.

It is vital for determining the strength of the encrypted images where some key parameters and encryption steps should be included. All the tests are reported with statistical analysis and sensitivity test that confirms the efficacy and security of the proposed technique in testing. Henon map-based dual cryptography is more efficient and offers better security features, such as faster processing, greater complexity, and stronger computational capabilities, when compared to single-layer encryption methods. Its benefits over traditional approaches include improved resistance to attacks on the encrypted image and a broader key space for analysis [12].

2.3. Henon map and its chaotic nature

Henon Map is two-dimensional mathematical function, first introduced in 1976 showing chaotic behavior when certain constants are used. It was derived from a two-dimensional map which is a Poincaré section of the Lorenz process with parameter values [6]. The Henon Map produces complexity and this is through the use of state equations. Due to large fluctuations in the number of digits, it is perfect for producing pseudo-random sequences needed in image encryption. Since the map is sensitive to the inputs, nonlinear, predictable, and easy to reconstruct when filling an image all make it efficient in this function [7]. In encryption, the chaotic properties of systems like the Henon Map feature a big role to play. They enhance issues such as randomness, system sensitivity to initial conditions, and the leading effects of parameters, all of which increases the security of image encryption [13]. These features assist to develop powerful secret keys by means of confusion-diffusion postulates. Due to this, chaos makes it possible for encrypted images not to be compromised, accessed or manipulated by unauthorized individuals [14].

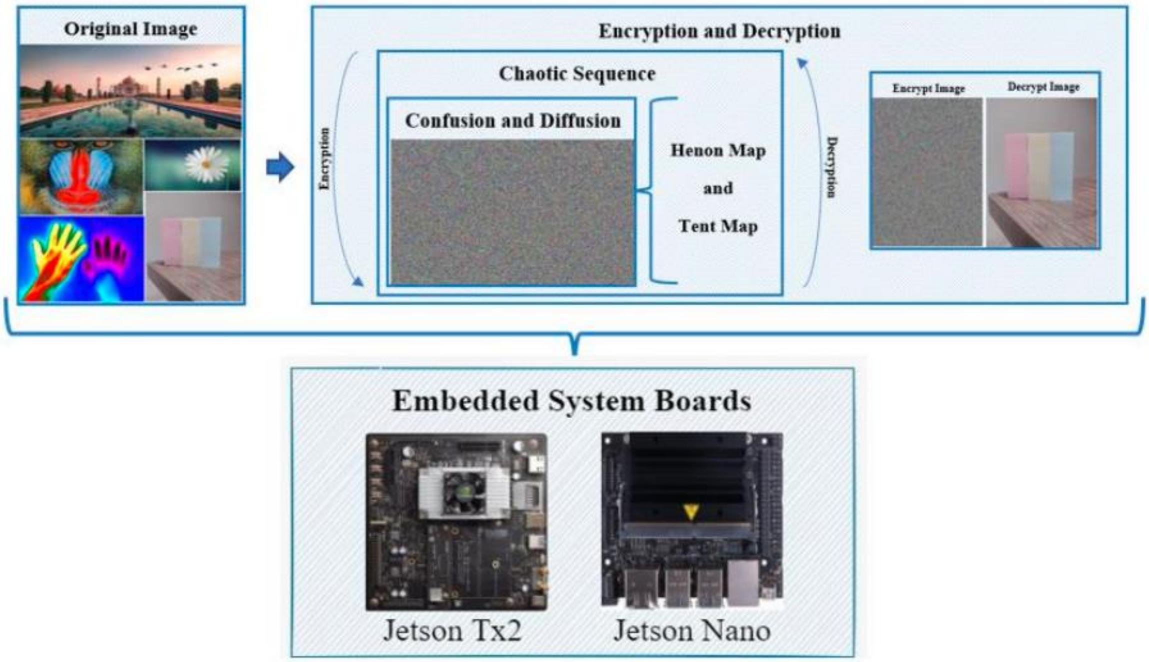

Fig. (2): An overview of the study (source: reference (DUFBE, 2023)) [16].

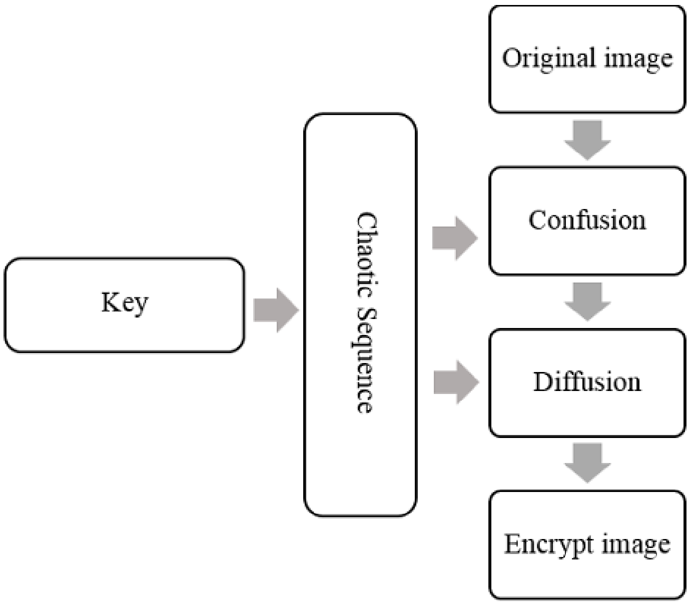

Fig. (3): Architecture of an image cryptosystem based on chaos (source: reference (DUFBE, 2023)) [16].

For instance, if use in combination with pixel shuffling or diffusion processes, the Henon chaotic system turns out to be a very efficient method for image encryption. Reported research shows that when using the Henon Map, entropy is high and the coefficients of the encrypted images not correlated as mentioned above, therefore the gray value distributions of these encrypted pictures are made more random [15]. (as demonstrated in Figures (2) and (3)).

Therefore, having been described the complex topological structure of the Henon Map, it can be said that the main advantage of the map for achieving high level of security for image encryption is the disorder. These aspects give protection against a number of other security risks that basic, more straightforward, single layer encryption mechanisms may not be equipped to combat [2].

2.4. Dual-layered cryptographic framework

Applying the concept of Henon map in a dual layered system is one of the most mature methods to enhance the security of the image used in digital communication. This new encryption technique uses chaotic systems like the Henon map to develop a two-stage approach that combines confusion and diffusion processes [6].

At this stage, the vulnerability of the original image is enhanced via using a modified Henon map that applies the image distortion in rounds for some times. The second layer utilizes chaotic image diffusion according to Henon map and enhances the security and makes the image highly resistant to attacks [13].

The main benefit of this two-layer cryptographic system is fast speed of cryptographic transformation together with high level of protection, which refers to a few most protected methods at the moment [14]. In the present case, by increasing the size of the secret key, it becomes quite difficult for the attackers to decrypt the images. This method of encryption has been found be useful through tests and the results of the image encrypted through this method have high entropy and low correlation of their coefficients thus making this encryption method powerful [11].

Single layer cryptographic systems also have some of the drawbacks explained below that the current advanced style of employment of the dual-layer cryptographic system thus effectively resolves. It makes it even more secure since it follows a two-step procedure. The characteristics of the chaotic motion of the Henon map and other theoretical concepts cause this method to rise above single-layer ones. Multiple layers provide far better protection against brute force attacks as well as other means of decrypting the images [8].

Therefore, adopting the Henon map in a two-fold cryptographic set for image protection is an important development in encryption instruments. The major advantage of such an approach is that it resulted delivery of significantly better protection and security to digital images [12]. The system can also produce multidimensional keys and has optimum security against all sorts of attacks on encrypted images as we require for image encryption in the present world [10].

2.5. Key parameters and encryption stages

Henon map is essentially better known for chaos nature of its dynamics this makes the given map rather stochastic. This quality is indispensable to drive the generation of important parameters in image encryption and consequently the process's security and resistance to attacks [13]. Because of its chaotic character, the Henon map exhibits high contractivity, and hence can be used as a source of stochastically chosen key parameters. Besides, the utilization of the Henon map assists in increasing the creation of a large key space and, therefore, enhances security. Hence a brute force would require an immense amount of computation [15].

The encryption system is based on double-layered chaotic maps and has been used alongside traditional ciphers for image encryption [11]. The first stage preliminary random sequences caused by the Henon map, and other chaotic maps, are used for rearranging pixels and XOR bitwise operation. This step of adds a great deal of randomness and non-linearity and thus it is difficult for any intruder to decode the images unless he or she knows the keys produced by the chaotic maps. In the second stage the classical encryption system such as the Hill cipher are employed for substitution and further, by incorporating different methods of cryptography [9].

In conclusion, this approach incorporates such chaotic maps as the Henon map, among other methods to enhance and protect image encryption since it is very powerful and secure [4].

2.6. The proposed system

This pseudocode describes a process for encrypting an image by generating two keys using the Henon map. The encryption works by using a substitution function that applies an XOR operation to the image elements with both keys in two rounds—first with key1 and then with key2. To decrypt the image, the process is reversed: the encrypted image is XORed first with key2 and then with key1, using the same substitution function.

```
function load_image(image_path):

  // Load the image from the specified path

function henon_map(params, iterations):

   // Generate key1, key2 using the henon map

   Return key1, key2

function bitwise_xor(array1, array2):
```

// Perform bitwise XOR operation between corresponding elements of two arrays

function save_image(image, path):

// Save the image to the specified path

function encrypt_image(image_path, henon_map_params):

original_image = load_image(image_path)

image_size = analize_image(original_image)

key1, key2 = henon_map (henon_map_params, image_size)

encrypted_image1=bitwise_xor (original_image, key1) encrypted_image2=bitwise_xor (encrypted_image1, key2) save_image(encrypted_image2, 'cipher_image.jpg')

function decrypt_image(image_path, henon_map_params):

original_image = load_image(image_path)

image_size = analize_image(original_image)

key1, key2 = henon_map (henon_map_params, image_size)

decrypted_image1 = bitwise_xor(original_image, key2)

decrypted_image2 = bitwise_xor(encrypted_image1, key1)

save image (decrypted_image2, 'decrypted_image.jpg')

function analyze image(original image):

// Analyze the image and extract relevant properties

// Properties may include size, color distribution, entropy, etc.

return size

function main ():

image path = 'path_to_your_image.jpg'

// Parameters of Henon map (x, y, a, b)

encrypt image (image path, { 'x': 0.001, 'y': 0.2, 'a': 1.4, 'b': 0.3 })

// To decrypt the encrypted image

CDX decrypt image ('cipher_image.jpg', { 'x': 0.001, 'y': 0.2, 'a': 1.4, 'b': 0.3 })

3. Results and Discussion

3.1. Presentation and analysis of results

The possibility of the second level of encryption and the level of guarantees provided by a two-tier cryptographic method based on the Henon map when protecting images were considered by presenting the results of experience. This approach was examined in relation to methods used for securing images, such as single layer encryption methods. In 2004, a NULL cipher methodology was employed for image encryption based on the dual layer of the Henon map; in doing so, an extra defense layer was introduced into the execution of the map [7].

The experimental assessment process involved quantifying a number of performance parameters like PSNR and NPCR and UACI along with histogram as well as computation time. The evaluation summary is provided in table 1, which allowed to determine the reliability and efficiency of the dual-layer cryptography system based on the Henon map [11].

The above simulation suggested that the present double-layer encryption system performs far better than single layer encryption/decryption techniques for comparable key sizes and the use of Henon map makes it more resistant to both, the differential and chosen plaintext attacks. The proposed 2-D hybrid chaotic map delivered superior NPCR and UACI values and better immunity against diverse attacks. Furthermore, The work is remarkable for the high computational efficiency of the Arnold cat map described in the publication [3].

Table 1: MSE and PSNR results of the test images using the proposed schemes. [23]

Images	Size	MSEOC	MSEOD	PSNROC	PSNROE
CT	512 × 512	17124.0626	0	5.7947	∞
MRI	512 × 512	16892.8865	0	5.8538	∞
Ultrasound	512 × 512	13338.4275	0	6.8798	∞
X-ray	1024 × 1024	10290.1876	0	8.0066	∞
CT-kidney	1024 × 1024	10039.2025	0	8.1138	∞

Table 2: Difference rates of two encrypted images with slight change in a parameter. [9]

Initial value	Changed value	Encrypted images difference rate
6	7	99.59%
2	1	99.60%
2	1	99.62%
12345678	12345679	99.58%
87654321	87654320	99.62%
12345	12346	99.63%

67890	67891	99.60%
1.21000001	1.21	99.59%
0.36000001	0.36	99.60%

Besides, parameters of the encrypting and decryption processes were critically evaluated together with key phases to confirm that dual-layer cryptography facilitated by the Henon map would enhance security in transferring images through networks. This was illustrated by encrypting two images as shown in Table 2.

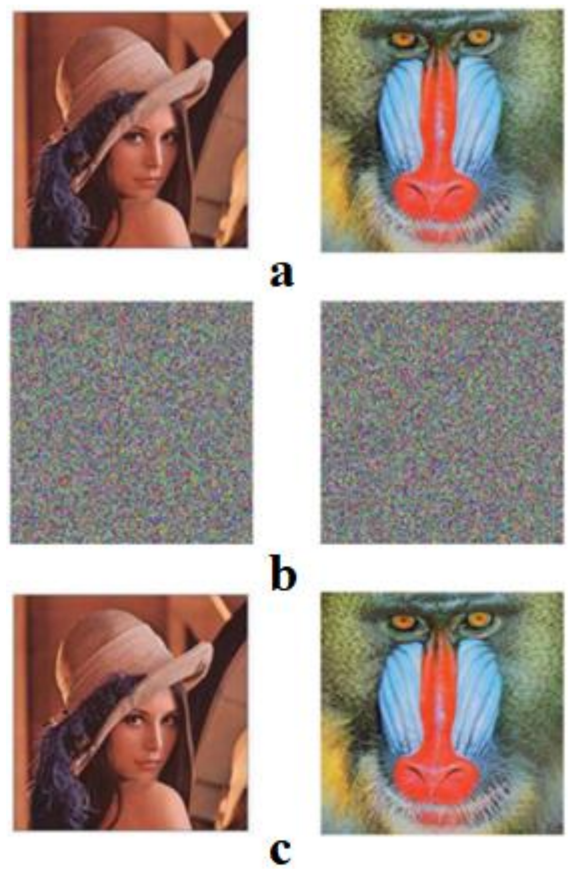

Fig. (4): Simulation results [4]: (a) Original Images (b) Encrypted Images (c) Decrypted Images

The suggested approach was significantly more efficient than the single-layer encryption algorithms regarding factors such as the immunity to statistical attacks and image characteristics after encryption [17], as shown in Figure (4).In conclusion, the experimental results indicate that a dual-layer cryptography approach based on the Henon map provides better protection and reliability for secure image transmission. It outperforms single-layer encryption methods in several key areas, making it a promising technique for strengthening image security.

3.2. Comparison with traditional single-layer encryption methods

It is, therefore, essential to compare the Two-Fold Cryptography Approach to the other traditional single-layer encryption techniques. Techniques such as AES, DES, and RSA have been employed for quite some time in the protection of data in digital form including images. However, these methods become a problem when it comes to the encryption of large multimedia files with strong pixel correlation. Dealing with chaos theory in cryptography has for the first time presented new techniques that are better suited to these challenges [19].

Chaos-based encryption techniques have proven to be more efficient in terms of security and efficiency than the commonly used techniques. chaos maps have some unique features such as, sensitivity to initial conditions, unpredictability, and randomness, which make it suitable for secure image encryption. Other researchers have shown that chaos-based encryption systems do actually satisfy Shannon's parameters of confusion and diffusion and thus help to form highly secure systems.

Also, it has been found that the security properties of chaos-based encryption algorithms are as good as those of modern encryption techniques. By making these comparisons, it has been possible to show the performances of some of the identified chaos-based algorithms in comparison to the traditional methods. For example, if given a security image through the Henon map, different attacks have proved to be unable to penetrate the system and are far more secure than traditional encryption procedures [8].

Another advantage that can be associated with the set of proposed chaos-based encryption techniques is the increased level of protection due to confusion and diffusion processes repeated many times. Such operations assist in combining the statistical features of the original image and the encrypted data so that the cryptanalysts cannot penetrate the concocted security system easily. Moreover, the integration of the chaotic maps with conventional cryptographic methodologies has given way to novel encryption techniques with more strings in security [3].

Thus, another major benefit of using chaos based encrypting techniques is the higher level of security provided by confusion and diffusion operations in several stages. These operations enable the mixing of the statistical characteristics of the original image with the encrypted data, making it harder for cryptanalysts to break the system. Additionally, combining chaotic maps with traditional cryptographic algorithms has led to new encryption solutions that provide higher levels of security [20].

In summary, comparing the Two-Fold Cryptography Approach with single-layer encryption techniques highlights the potential benefits of using the Henon Map for image security. Combining chaotic systems with traditional encryption methods offers a promising way to strengthen image security while overcoming the limitations of conventional approaches.

4. Conclusion

The use of a dual encryption method based on the Henon Map showed a high degree of complexity and efficiency in image security. We observe that the pixel diffusion index is very high, getting an excellent correlation and entropy index. A unique key scrambling method, which we incorporate, tends to distribute the pixels evenly over the image. Finally, this has shown the stability of the developed system through sets of 15 different experiments with distinct datasets, as well as the evaluation of multiple performance criteria. Additionally, it is scalable to any number of channels and key lengths, so it is particularly flexible in a multitude of scenarios [8].

An advantage associated with our proposed method is that there is likely to be reduced traffic on the transmission channel while at the same time enhancing the security aspect of the channel. This results in an accelerated time of encryption and fewer bandwidth units required in transmitting the encrypted image. The shorter transmission time and the smaller file size both contribute to improving the method's efficiency. As for the level of encryption implemented our system has performed well even in comparison to seemingly unrelated concepts across numerous indicators which attests to its effectiveness and adaptability [21].

Thus, the results are stronger, though our goal for further research is to achieve the optimal levels for these indicators. In future work, it is planned to apply the created system with hyperspectral images and evaluate the quality of results on various images.

Therefore, the use of the two cryptographic methods based on the Henon Map indicates a promising future in image security. The one-way key scrambling process and the fast encryption procedure also qualify it for suitable application in areas where secure data transmission is relevant [22].

Acknowledgment: Not applicable.

Generative AI

During the preparation of this work the authors used [QuillBot] in order to rephrase and increase clarity of some sections in introduction. After using this tool, we reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

[1] Shariatzadeh, M., Eftekhari, M., Rostami, M. J., 2022, A New Scheme for Image Compression and Encryption Using ECIES, Henon Map, and AEGAN, Preprint. https://arxiv.org/pdf/2208.07635

[2] Alani, D. S., Al Iesawi, S. A., 2018, Image Encryption Algorithm Based on Rc4 and Henon Map, Journal of Theoretical and Applied Information Technology, 6(21). http://www.jatit.org/volumes/Vol96No21/7Vol96No21.pdf

[3] Rehman, M. U., Shafique, A., Khan, K. H., & Hazzazi, M. M., 2023, Efficient and secure image encryption using key substitution process with discrete wavelet transform, Journal of King Saud University - Computer and Information Sciences, 35(7), 101613. https://doi.org/10.1016/j.jksuci.2023.101613

[4] Wang, L., Ran, Q., & Ding, J., 2023, Image encryption using Quantum 3D mobius scrambling and 3D Hyper-Chaotic Henon Map. Entropy, 25(12), 1629. https://doi.org/10.3390/e25121629

[5] Salman, D. S., & Naif, J. R., 2023, COMPARATIVE STUDY OF CHAOTIC SYSTEM FOR ENCRYPTION, Iraqi Journal for Computers and Informatics, 49(2), 83–92. https://doi.org/10.25195/ijci.v49i2.457

[6] Chaudhary, N., Neupane, A., TeChaudhary, N., Shahi, T. B., & Neupane, A., 2022, Secure image encryption using chaotic, hybrid chaotic and block cipher approach, Journal of Imaging, 8(6), 167. https://doi.org/10.3390/jimaging8060167

[7] Sankhe, P., Pimple, S., Singh, S., LahaneFu, A., 2018, sawq1` An Image Cryptography using Henon Map and Arnold Cat Map, International Research Journal of Engineering and Technology (IRJET), 5(4), 1900. www.irjet.net.

[8] Kanwal, S., Inam, S., Ben Othman, M. T., Waqar, A., Ibrahim, M., Nawaz, F., Nawaz, Z.,, Hamam, H., 2022, An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices. PubMed Central, 22(12), 4359. https://doi.org/10.3390%2Fs22124359

[9] Nkuigwa, G. G. G., Nzeuga, H. D., Fouda, J. a. E., Sabat, S. L., & Koepf, W., 2022, An extendable key space integer image-cipher using 4-bit piece-wise linear cat map. Multimedia Tools and Applications, 82(10), 14609–14631.

https://doi.org/10.1007/s11042-022-13779-y

[10] Zhao, Y., & Liu, L., 2021, A bit shift image encryption algorithm based on double chaotic systems, Entropy, 23(9), 1127. https://doi.org/10.3390/e23091127

[11] Kanwal, S., Inam, S., Othman, M. T. B., Waqar, A., Ibrahim, M., Nawaz, F., Nawaz, Z., & Hamam, H., 2022, An effective color image encryption based on Henon Map, Tent Chaotic Map, and orthogonal matrices. Sensors, 22(12), 4359. https://doi.org/10.3390/s22124359

[12] Shrivastava, D., Bagoria, R., Vidyarthi, A., 2023, Image Encryption Algorithm Based on Chaos Cryptography, Survey. GIS SIENCE JOURNAL, 10(1), 776. https://gisscience.net/wp-content/uploads/75-GSJ9606.pdf

[13] Mfungo, D. E., Fu, X., Xian, Y., & Wang, X., 2023, A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information. Applied Sciences, 13(12), 7113. https://doi.org/10.3390/app13127113

[14] Afifi, A., 2019, A chaotic Confusion-Diffusion image encryption based on Henon Map, Social Science Research Network. https://doi.org/10.2139/ssrn.3439189

[15] Mishra, K., Saharan, R., 2019, A Fast Image Encryption Technique Using Henon Chaotic Map: Proceedings of ICACIE 2017, 1. https://doi.org/10.1007/978-981-13-1708-8_30

[16] CANDAN, Ç., SAHIN, M. E., 2023, Implementation of Real-Time Image Encryption Using Chaotic Maps in Embedded Systems. Düzce University Journal of Science & Technology, 11, 2023, 1037-1047. https://doi.org/10.29130/dubited.1159078

[17] Nejad, M. R., & Fartash, M., 2016, APPLYING CHAOTIC IMPERIALIST COMPETITIVE ALGORITHM FOR MULTI-LEVEL IMAGE THRESHOLDING BASED ON KAPUR'S ENTROPY. Advances in Science and Technology Research Journal, 10(29), 125–131. https://doi.org/10.12913/22998624/61940

[18] Li, S., Zhao, L., & Yang, N., 2021, Medical image encryption based on 2D zigzag confusion and dynamic diffusion. Security and Communication Networks, 2021, 1–23. https://doi.org/10.1155/2021/6624809

[19] Soleymani, A., Nordin, J., & Sundararajan, E., 2014, A chaotic cryptosystem for images based on Henon and Arnold Cat map. The Scientific World Journal, 2014, 1–21. https://doi.org/10.1155/2014/536930

[20] Lone, P. N., & Singh, D., 2020, Application of algebra and chaos theory in

security of color images. Optik, 218, 165155. https://doi.org/10.1016/j.ijleo.2020.165155

[21] Hassan, S. S., Iqbal, Z., Ikram, M.J., Ishaque, M., 2022, Henon Chaotic Map Based Image Encryption Scheme Using Bit-Level Circular Shift. Journal of Theoretical and Applied Information Technology, 100. 6, 1960. http://www.jatit.org/volumes/Vol100No6/31Vol100No6.pdf

[22] Uddin, M. R., Jahan, F., Islam, M. K., & Hassan, R., 2021, A novel DNA-based key scrambling technique for image encryption. Complex & Intelligent Systems, 7(6), 3241–3258. https://doi.org/10.1007/s40747-021-00515-6