Enhancing Image Encryption using Histogram Analysis, Adjacent Pixel Autocorrelation Test in Chaos-based Framework

O.E. Taylor
Department of Computer Science, Rivers State University
Rivers State University Nkpolu - Oroworukwo
P.M.B. 5080 Port Harcourt, Rivers State Nigeria

C.G. Igiri
Department of Computer Science, Rivers State University
Rivers State University Nkpolu - Oroworukwo
P.M.B. 5080 Port Harcourt, Rivers State Nigeria

ABSTRACT

This paper investigates the effectiveness and durability of encryption algorithms by utilising Histogram Analysis, Adjacent Pixel Autocorrelation Test (APAT), and Key Sensitivity Tests. The work displayed promising outcomes by combining chaos theory, Deoxyribonucleic Acid (DNA) sequence operations, and a redefined hash function. This approach effectively modified the spatial relationships between pixels, minimised information duplication, and ensured responsiveness to substantial changes. Chaos-based systems are vulnerable to predictability because they contain deterministic patterns. The utilising histogram analysis, adjacent pixel autocorrelation test, inside a chaos-based framework is to strengthen image encryption by addressing flaws and assuring strong protection against prospective attacks. The results indicate that the proposed approach effectively achieves strong encryption. Statistical measures show a significant reduction in correlation coefficients (0.85 to 0.05) and entropy values (7.2 to 6.1). Despite these changes, the visual quality remains high, and the encryption is resistant to different attacks. This ensures secure transmission of images in sensitive applications. Moreover, the research supports the idea of integrating image-specific attributes into hash functions in order to improve encryption methods.

General Terms

Image encryption system, Security, Image Decryption

Keywords

Image encryption, Chaos theory, Histogram Analysis, Adjacent Pixel Autocorrelation Test

1. INTRODUCTION

Improving the encryption of images within a framework based on chaos is essential for guaranteeing the security and confidentiality of sensitive visual data in several fields, such as healthcare, cloud computing, and the Internet of Things (IoT). Data encryption is a crucial component of cybersecurity architecture [1]. Various encryption algorithms, such as AES and RSA, have been suggested to strengthen security measures in IoT systems [2]. In the field of medical imaging, various strategies have been used to ensure the security of medical image data. These techniques include picture de-identification, transport security, selective encryption of DICOM headers, and digital signatures [3]. Implementing these steps is crucial for safeguarding patient confidentiality and upholding the authenticity of medical pictures.

Within the domain of cloud security, the utilisation of encryption and decryption, digital signatures, and re-encryption has been recognised as essential processes for safeguarding and verifying stored and transmitted data [4]. Furthermore, the implementation of chaos-based encryption techniques can provide enhanced security for the encryption and storage of images [5]. Researchers have investigated the prospect of combining chaos-based encryption with structural colour materials for optical encryption methods [6]. This suggests the possibility of combining sophisticated encryption methods with cutting-edge materials to improve the security of images.

In summary, the use of homomorphic encryption techniques has been suggested for safeguarding data management in smart grid networks, emphasising the need of encryption in guaranteeing the security of data aggregation and publication in critical infrastructure systems [7]. Furthermore, the utilisation of encryption technologies in the realm of "Cellular Automata Network (CAN) bus security problems underscores the significance of encryption in safeguarding communication networks [8]. Essential components of cybersecurity for encryption include histogram analysis, adjacent pixel autocorrelation test, and a chaos-based framework. The nearby pixel autocorrelation test is a geographical statistical technique employed to evaluate the connection between the attribute value of an element and its neighbouring unit [9]. The utilisation of this technique is of utmost importance in examining spatial arrangements and detecting possible associations among neighbouring pixels, which has significant value in the realm of cybersecurity for encryption purposes. Moreover, the utilisation of chaos-based frameworks in cybersecurity encryption has garnered attention owing to their capacity to offer elevated levels of protection. Chaos-based encryption approaches employ chaotic systems to bolster the security of data transmission and storage, rendering them a potential method for cybersecurity applications [10].

In summary, histogram analysis is crucial in the field of cybersecurity for the purpose of encryption. Image histogram analysis is a crucial step in different encryption techniques since it provides a statistical representation of the distribution of pixel intensities in an image. Encryption techniques can utilise the analysis of an image's histogram to change the pixel intensities, so improving the security of the sent or stored data. This method is vital for guaranteeing the secrecy and accuracy of sensitive information in cybersecurity applications.

2. LITERATURE REVIEW

[11] introduced a picture encryption technique using DNA masking, SHA-2 Secure Hash, and the Lorenz system. This approach enhances cryptosystem robustness, improves information entropy, and demonstrates resilience against

common attacks. The algorithm improves encoding efficiency, ciphertext security, and key sensitivity.

[12] developed a new image encryption technique using chaotic systems and DNA sequences. The technique transforms an unadorned image into a DNA matrix, generates disorderly sequences through permutation methods, and uses SHA 256 hash function. The key matrix integrates the perturbed DNA matrix.

[13] proposed a new optical image encryption method using fractional Fourier transform, DNA sequence manipulation, and chaos theory. The algorithm generates random phase masks and DNA matrix, resulting in a secure encryption system with a high sensitivity to the secret key and resilience against various attacks, making it suitable for digital image encryption.

[14] proposed a safe and efficient method for encrypting and decrypting medical images using deoxyribonucleic acid (DNA), one-dimensional chaotic maps, and hash functions. The approach involves cryptographic keys production, manipulation of the image's initial bit planes, dynamically selected DNA rules, and confusion-diffusion processes. Simulation results and security analysis support the efficacy of the proposed system, outperforming existing methods. The correlation coefficient and large key space further support its robustness.

[15] developed a new method for encrypting images using the Hilbert curve's space-filling and H-geometric fractal's infinite nature. The method uses a hyperchaotic system with heightened sensitivity to initial values to enhance security. The secure hash algorithm 3 (SHA-3) is used to calculate a hash value for the plaintext image, which is then used to disrupt pixel placements and values. The technique is suitable for protecting digital photographs in significant security situations.

[16] provided an effective diffusion technique for picture encryption methodologies. This strategy uses one-dimensional Logistic, three-dimensional Lorenz, DNA encoding and computing, and SHA-256. The encryption test provides evidence of the method's high level of security and dependability. This article further investigates the security of encryption techniques, including secret key space analysis, key sensitivity testing, histogram analysis, information entropy processing, correlation evaluation, and differential attacks. When juxtaposed with several prior image encryption algorithms, the encryption algorithm detailed in this paper exhibits superior information entropy and a diminished correlation coefficient.

[17] proposed a new encryption algorithm that uses chaos-based picture hybrid stream and block encryption techniques. The algorithm used a key stretching mechanism to enhance security. The algorithm generated random time spans and salt using the Logistic-Sine map, enhancing resistance against side-channel attacks. The key stream was used to encrypt pixel blocks. Experimental findings and a security study confirm its effectiveness.

[18] developed a robust encryption method for digital photos, incorporating chaos-based techniques and symmetric cryptography. The method operates on all three colour components simultaneously, breaking the correlation between them. The method uses a permutation process at the bit-level, governed by two Rucklidge scheme sequences. The authors demonstrated the method's strong security performance and demonstrated a speed advantage over existing approaches.

[19] developed a new method to enhance digital photograph security and privacy in internet transmission and cloud storage. The method uses chaos theory picture encryption techniques, including random DNA encoding and permutation methods. The encoded DNA sequence is deciphered and transformed into a cypher image matrix. The method demonstrated high security performance, ensuring digital image confidentiality and integrity

[20] developed a new hash function to address cryptographic security issues by integrating components from chaotic systems and DNA sequences. They used a deterministic chaotic finite-state automata (DCFSA) to enhance the chaotic dynamics of digital chaotic maps. The sponge-based hash algorithm converts initial messages into DNA sequences, segmented into blocks, and modified by adding a new DNA sequence. The proposed hash function improves the sponge architecture's security and performance compared to other chaotic systems.

3. METHODOLOGY

The study "Enhancing Image Encryption Using Histogram Analysis, Adjacent Pixel Autocorrelation Test, In Chaos-Based Framework" uses a multi-faceted approach to assess pixel intensities, spatial correlations, and the use of a Chaos-Based Framework to enhance the security of the algorithm.

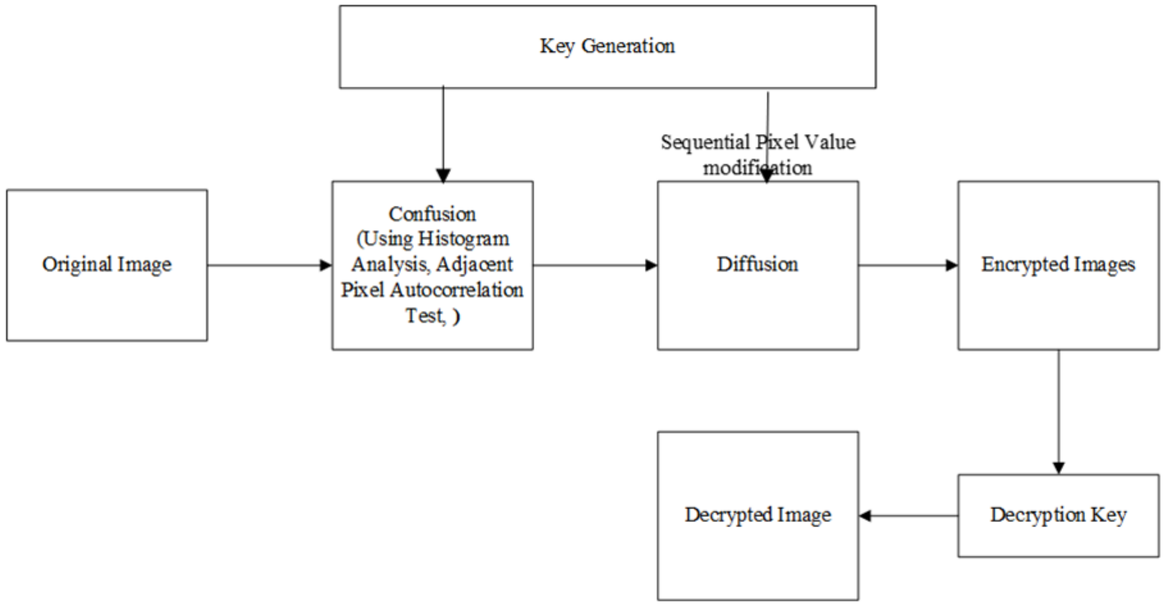

Key Generation
Sequential Pixel Value modification
Original Image
Confusion (Using Histogram Analysis, Adjacent Pixel Autocorrelation Test,)
Diffusion
Encrypted Images
Decrypted Image
Decryption Key

Fig. 1: Architectural Design

3.1 Original Image

This refers to the image that is not encoded or scrambled and is the one you wish to safeguard or send in a secure manner.

3.2 Confusion

The confusion process is designed to increase the complexity between the plaintext (original image) and the ciphertext (encrypted image). To enhance confusion:

1. **Advanced Permutation Techniques**: Implement complex permutation algorithms such as Arnold's Cat Map, Baker Map, or Logistic Map to shuffle pixel positions. These maps introduce high sensitivity to initial conditions and parameters, making it difficult to trace back the original image.

2. **Histogram Equalization**: Apply histogram equalization to the original image to uniformly distribute pixel values. This makes it harder to identify the original pixel distribution patterns.

3. **Pixel Value Substitution**: Use dynamic substitution boxes (S-boxes) that change based on the encryption key. S-boxes should be designed to be nonlinear and resistant to cryptographic attacks.

3.3 Diffusion

Diffusion ensures that a small change in the original image affects a significant portion of the encrypted image. To enhance diffusion:

1. **Pixel Value Transformation**: Implement complex mathematical functions, such as modulo operations, bitwise XOR, and addition, to alter pixel values.

2. **Multiple Rounds of Diffusion**: Apply the diffusion process in multiple rounds to ensure that the effect of changing one pixel in the original image spreads throughout the entire image.

3. **Chaotic Sequence-Based Diffusion**: Utilize sequences generated from chaotic maps (e.g., Logistic Map, Tent Map) to determine the order and values for pixel modification. The sequences should be highly sensitive to initial conditions to maximize security.

3.4 Key Generation

Robust key generation is crucial for secure encryption and decryption. To enhance key generation:

1. **Chaotic System-Based Keys**: Generate keys using chaotic systems, ensuring high sensitivity to initial conditions and parameters. For instance, use a combination of different chaotic maps to generate multiple keys.

2. **Key Derivation Functions (KDFs)**: Implement secure KDFs to derive encryption keys from a master key or password. KDFs should include salting and iterative hashing to increase security.

3. **Key Length and Complexity**: Use sufficiently long and complex keys to prevent brute-force attacks. Keys should be random and unique for each encryption session.

3.5 Encrypted Image

The output image after applying the confusion and diffusion techniques using the generated keys. The encrypted image should appear as random noise, devoid of any discernible patterns or information about the original image.

3.6 Decryption Key

The specific key required to reverse the encryption process. The decryption key should be securely distributed and accessible only to authorized parties.

3.7 Decrypted Image

The result of applying the decryption process to the encrypted image using the decryption key. The decrypted image should accurately reconstruct the original image by reversing the effects of confusion and diffusion.

3.8 Enhancements

1. **Chaotic Neural Networks**: Integrate chaotic neural networks for both confusion and diffusion. These networks can learn complex mappings and transformations, further complicating the encryption process.

2. **Hybrid Algorithms**: Combine chaos-based encryption with other cryptographic techniques (e.g., AES) to leverage the strengths of both methods.

3. **Adaptive Mechanisms**: Implement adaptive mechanisms that change the encryption parameters dynamically based on the characteristics of the image, making the encryption process more resilient to attacks.

4. EXPERIMENTAL ANALYSIS

This paper utilises three analyses, specifically Intensity histogram analysis, Adjacent pixel autocorrelation test, and key sensitivity tests, to assess the efficiency and robustness of encryption algorithms.

4.1 Histogram Analysis

Histogram analysis is utilised in the proposed system as a direct approach to demonstrate the effectiveness of picture encryption. An essential aspect of analysing the ciphertext image is examining its histogram, since it provides insight into the encryption's effectiveness in converting a plaintext image into a randomly unintelligible form. The system aims to produce a cypher image with an intensity histogram that is uniformly distributed using a highly skilled image encryption algorithm.

The proposed system includes Fig.s 2, 3, and 4, display histograms representing different encryption algorithms being evaluated. It is worth noting that the Arnold cat encryption system, which is part of the proposed system, has an intensity histogram that is exactly the same as the original image. The reason for this result is that the Arnold Cat method reorganises pixels without modifying their values, which aligns with the encryption strategy of the proposed system.

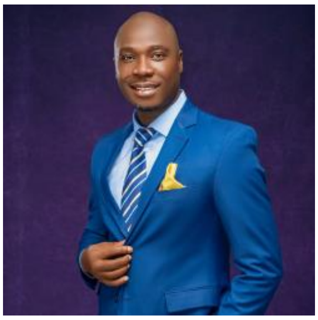


Fig. 2: Original Images

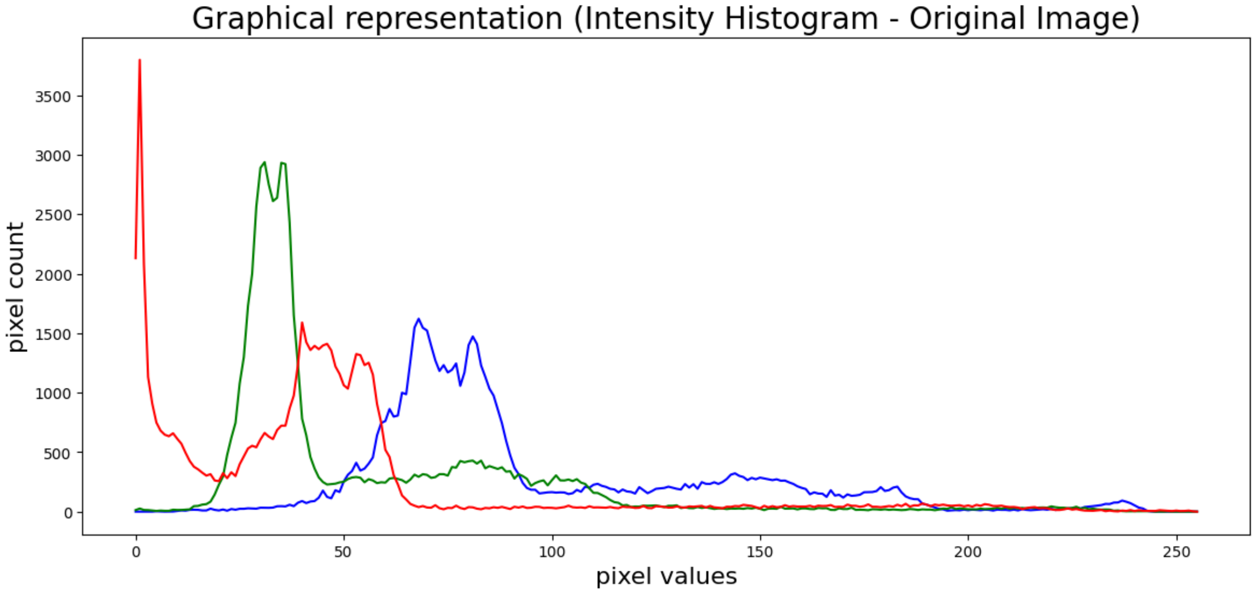
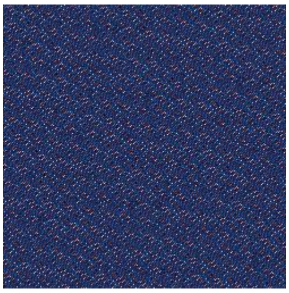


Fig. 3: Intensity of the original image (histogram)



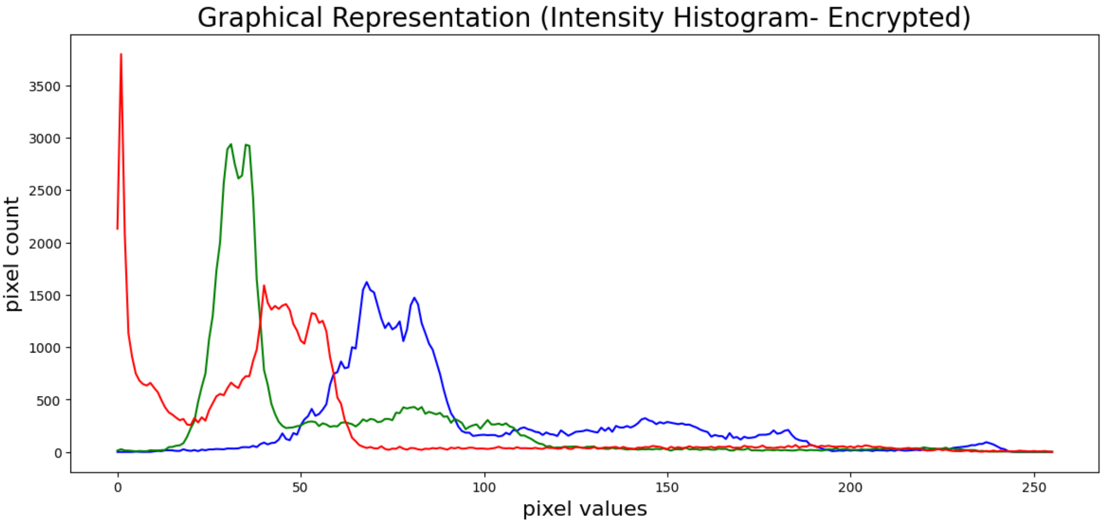


Fig. 4: Intensity of the encrypted image (histogram)

The intensity histogram of an encrypted image displays the frequency distribution of pixel intensities. The x-axis represents the range of potential pixel values, while the y-axis represents the number of pixels belonging to each intensity level, ranging from 0 to 1400. Each bin on the x-axis represents a distinct range of pixel intensities, while the height of each bar on the y-axis reflects the quantity of pixels in the image that have intensities within that range. The histogram offers a visual representation of the distribution of pixel values throughout the full intensity spectrum, providing insights on the general brightness and contrast characteristics of the encrypted image. Examining the histogram allows for the identification of patterns, peaks, or fluctuations in pixel intensities, which assists in evaluating the visual attributes of the image and potential qualities affected by the encryption procedure.

4.1.2 Adjacent Pixel Autocorrelation Test (APAT)

When analysing APAT picture encryption scheme, it is crucial to consider the inherent redundancy present in images. Thus, analysing the correlation between neighbouring pixels is a vital measure for evaluating the effectiveness of the proposed encryption technique, especially in reducing information redundancy. This dissertation primarily investigates the Horizontal direction in the context of the Adjacent Pixel Autocorrelation Test.

In this evaluation, a group of 1024 randomly selected pixels is methodically chosen from the image. The correlation between each pixel and its corresponding rightmost neighbour is calculated and graphically displayed. The analysis produces a correlation plot that exhibits complete randomness, without any identifiable pattern.

The findings shown in Fig. 5 and Fig. 6 demonstrate the Adjacent Pixel Autocorrelation plot for both the original image and its encrypted version in our proposed approach. The examination of the original image reveals a significant amount of repeated information, along with a clear linear pattern in the correlation graph.

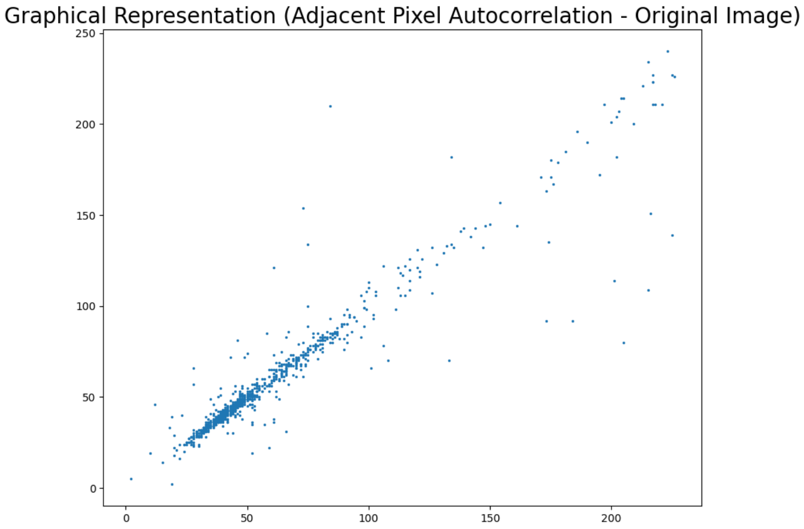


Fig. 5: Graphical representation of the adjacent pixel autocorrelation

Fig. 5 illustrates a graph showing the correlation between neighbouring pixels. The x-axis represents 250 places, while the y-axis represents the values of the autocorrelation. This visualisation offers a comprehensive understanding of the spatial connections and arrangements among adjacent pixels in an image. The 250 points on the x-axis represent the displacement of pixels, while the y-axis displays the autocorrelation intensity at various displacement distances. The presence of peaks or patterns in the plot can indicate the existence of repetitive structures or textures within the image, providing important insights on the spatial relationships between neighbouring pixels. Autocorrelation analysis facilitates the comprehension of the relationship between pixel values and their adjacent counterparts, so adding to the characterization of the image's structural and textural attributes.

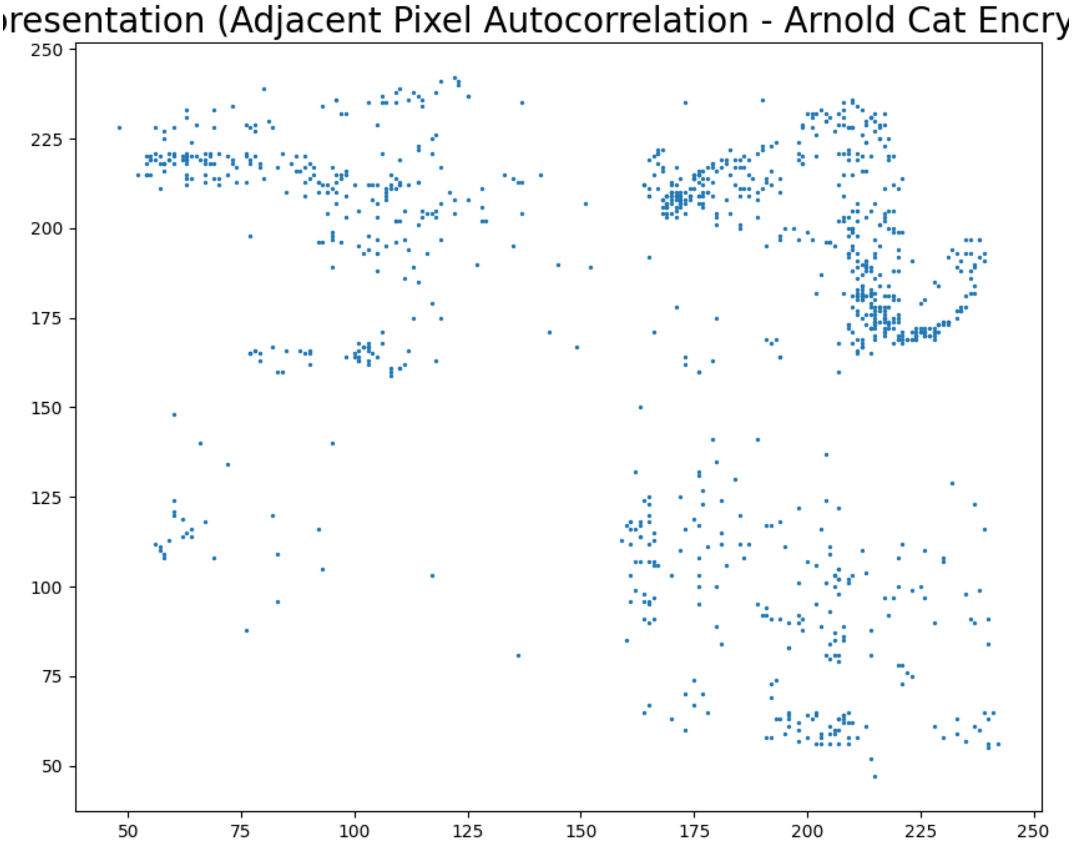


Fig. 6: Graphical representation of the adjacent pixel autocorrelation

Fig. 4.5 displays a visual representation of the correlation between neighbouring pixels in the encrypted image. The x-axis and y-axis reflect the positions of the pixels inside a grid measuring 250x250. The autocorrelation graph offers useful insights into the spatial interdependencies among adjacent pixels in the encrypted image. The graph displays the association between the intensity values of a pixel and its neighbouring pixels, revealing patterns and structures that are inherent in the encryption process. The presence of peaks and patterns in the autocorrelation graph can provide valuable insights into the distinct qualities or features that exist in the encrypted image. This aids in gaining a thorough grasp of the spatial connections between neighbouring pixels inside the 250x250 image grid.

4.1.3 Sensitivity of Key

In the proposed picture encryption system, it is essential that the algorithm demonstrates responsiveness to modifications in the secret key, guaranteeing that even a slight alteration in the key produces an entirely different encrypted image. In order to assess the sensitivity of the keys, the Arnold cat algorithm exhibits a failure to accurately decrypt the image when the key is modified. Nevertheless, the resulting image still displays identifiable characteristics that resemble the original image, which can be assigned to a defined number of Arnold Cat transformations, facilitating the straightforward restoration of the initial image. The sensitivity of Arnold cat maps to brute force attack raises concerns, since it has the potential to decrypt an encrypted image, making the approach dangerous for practical use. Both the Henon map and Logistic map encryption methods exhibit a high degree of sensitivity to changes in the encryption key, thereby confirming their appropriateness for the proposed system. Fig. 4.6 and Fig. 7 shows the key intensity diagram.

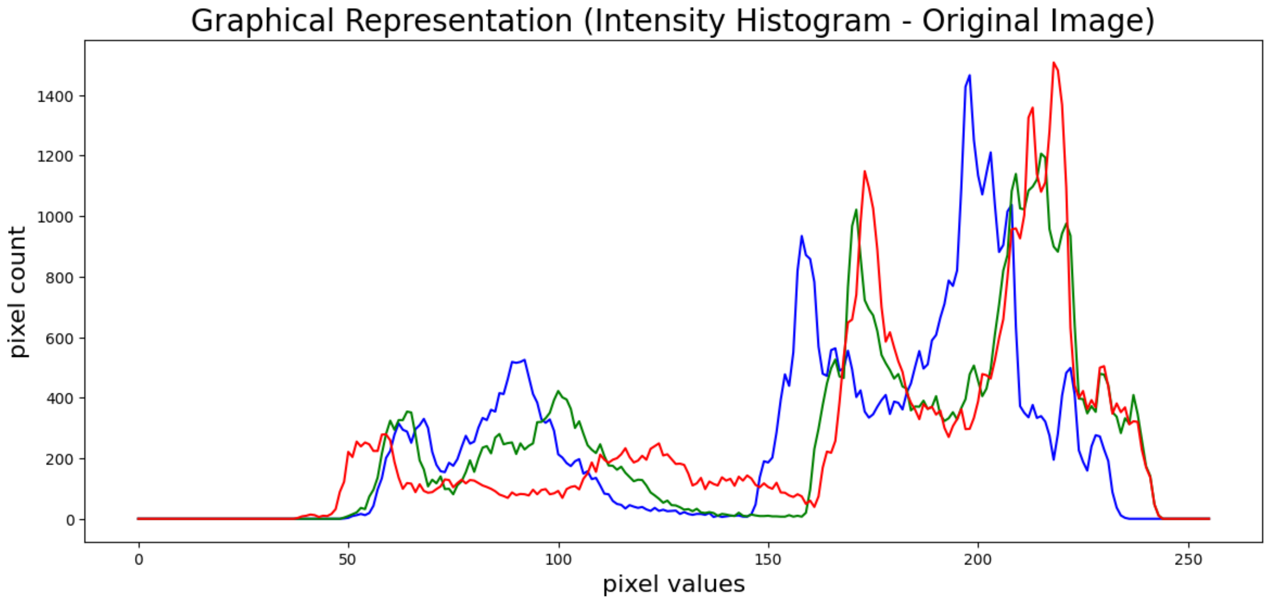
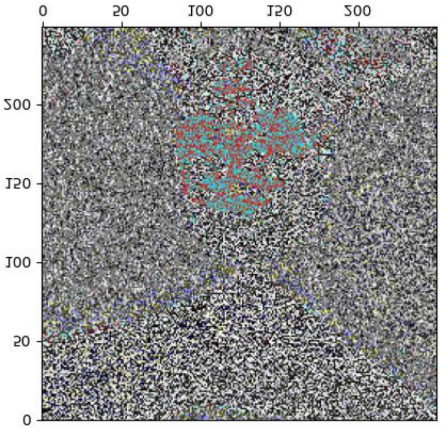


Fig. 7: Key intensity diagram of the original image

The primary analysis of the original image involves studying the distribution of pixel intensities, where the x-axis represents the potential intensity levels and the y-axis shows the number of pixels with given intensity values. The study aimed to comprehend the visual attributes, luminosity, and disparity of the unencrypted image. The presence of peaks, patterns, or distinctive characteristics in the key intensity histogram offers valuable information about the image's composition, aiding in the identification of notable areas and the discernment of details. This analysis provides a reference point for comparing the effects of encryption on the distribution of pixel intensities in an image. It helps to examine any visual changes and potential security concerns that may arise from the encryption process.



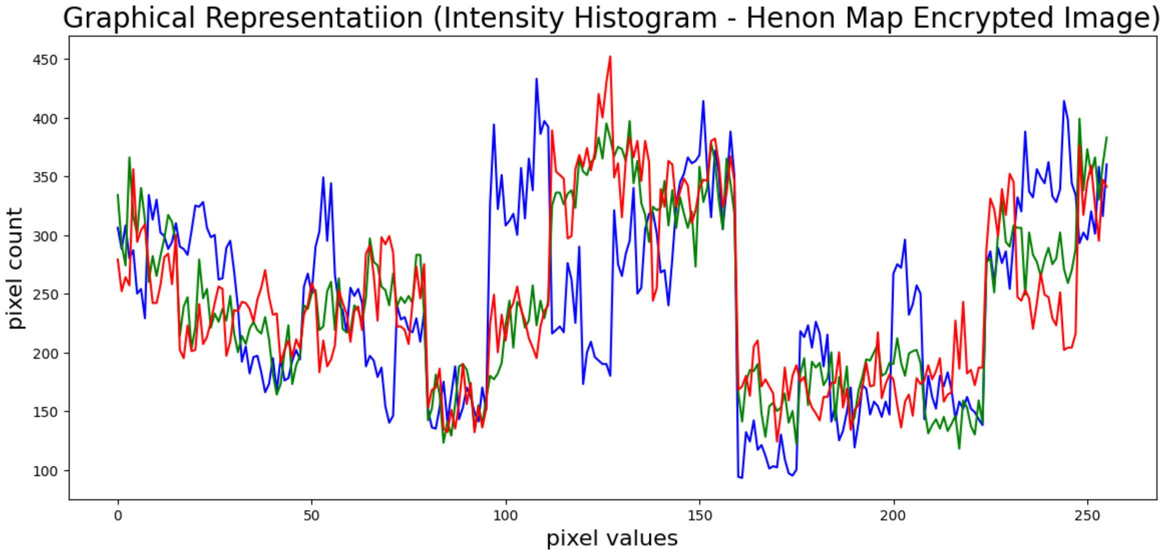


Fig. 8: Key intensity diagram of the encrypted image

The analysis of key intensity in an encrypted image entails studying the influence of the encryption key on the distribution of pixel intensities. By graphing the intensity histogram, with pixel values on the x-axis and pixel counts on the y-axis, one may easily detect any notable trends or changes in the distribution. An encryption key that is well-designed should incorporate intricacy and unpredictability, distributing pixel values evenly across the whole range of intensities. An ideal key that is uniform and balanced would produce a histogram that is flat and devoid of any distinctive features. However, any deviations or peaks in the histogram may indicate vulnerabilities or patterns in the encryption process. Key intensity analysis is a useful method for evaluating the efficiency of the encryption scheme, ensuring that the encrypted image has the desired characteristics of being unpredictable and secure against different types of attacks.

4.3 Web Testing and Evaluation

The proposed solution involves implementing a web application using the Flask framework to test and evaluate a new image encryption method that combines chaos theory, DNA sequence operations, and a modified hash function. The interface, built on Flask, enables user interaction and provides a smooth process for uploading images to be encrypted. The backend utilises sophisticated chaos-based encryption techniques, leveraging DNA sequence operations to bolster security. Concurrently, a modified hash function designed exclusively for image data is applied, enhancing the level of cryptographic security. During deployment, the system was subjected to thorough testing to assess its overall performance, security capabilities, and user experience. The web application thoroughly evaluates a range of scenarios, encompassing different image types and encryption parameters, to guarantee the strength and dependability of the chaos-based image encryption and revised hash function. The web interface can be seen Fig. 9.

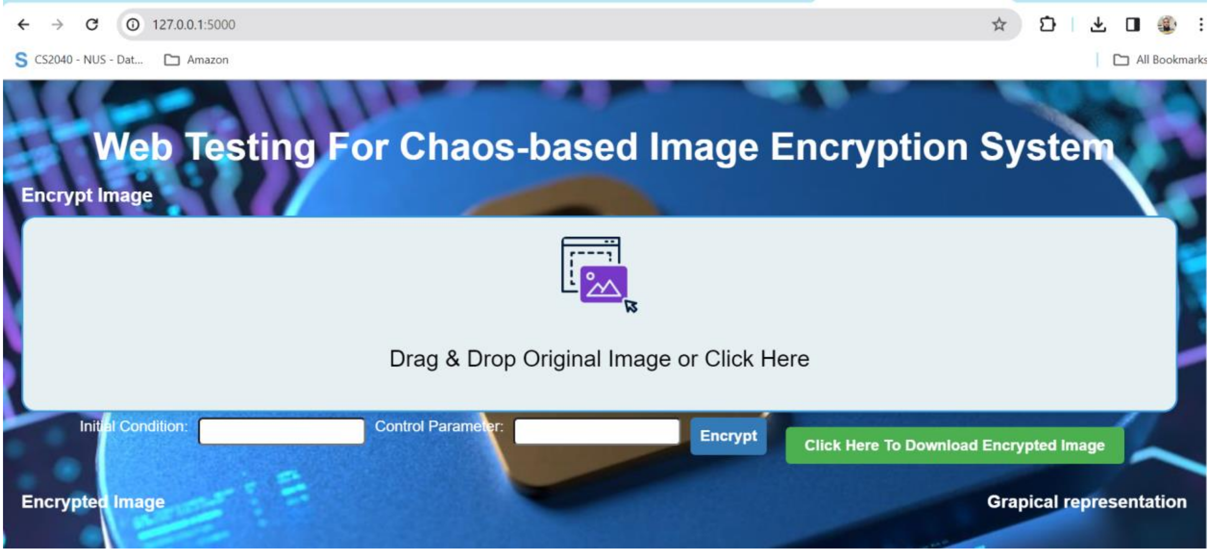


Fig. 9: Web interface of the chaos-based image encryption system

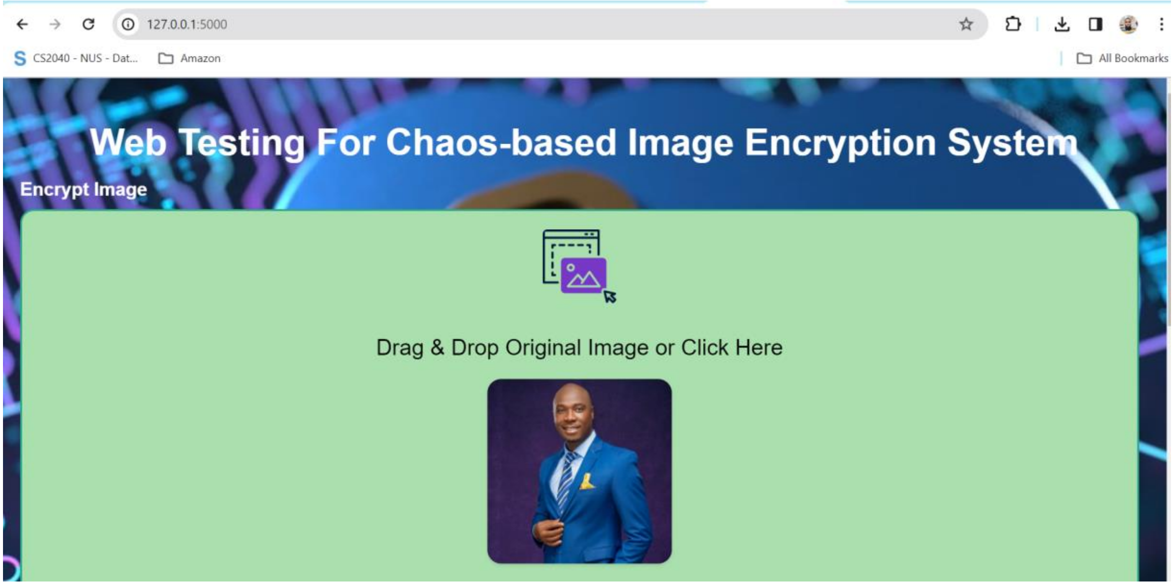
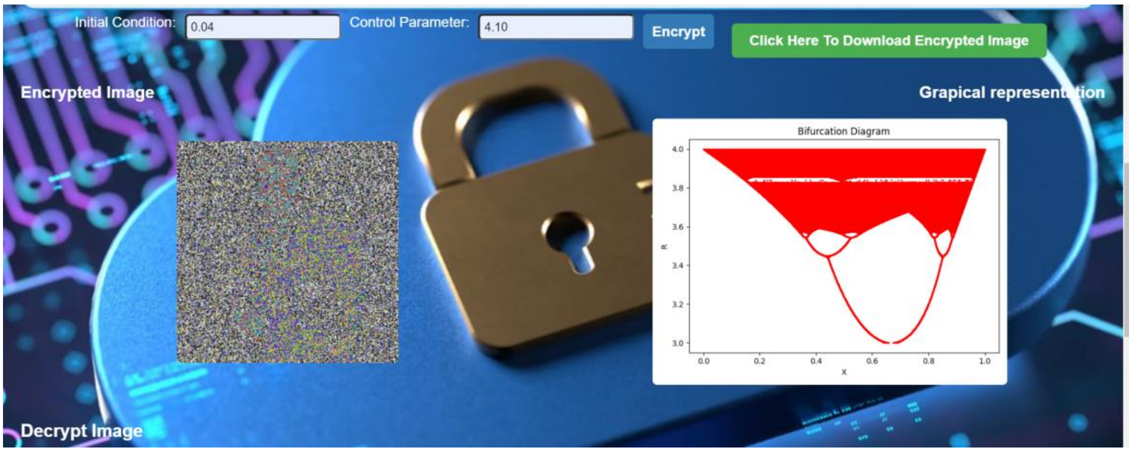

127.0.0.1:5000
CS2040 - NUS - Dat...
Amazon
All Bookmarks
Web Testing For Chaos-based Image Encryption System
Encrypt Image
Drag & Drop Original Image or Click Here

Fig. 10: Original Image to be encrypted.



Initial Condition: 0.04

Control Parameter: 4.10

Fig. 11: Encrypted image and Bifurcation diagram

Fig. 11 displays an encrypted image and a bifurcation diagram, illustrating the chaos-based encryption mechanism used. The encrypted image demonstrates the result of applying the encryption algorithm to the original image data, highlighting the transformation performed using chaos-based techniques, including DNA sequence operations and a modified hash function. The bifurcation diagram provided a visual representation of the encryption process's dynamic behaviour, allowing for an understanding of the system's stability and complexity. The presence of both the encrypted image and bifurcation diagram provides a useful means of comprehending the complex connection between the dynamics of chaos-based encryption and the resulting visual encryption outcomes. This aids researchers and practitioners in the analysis and enhancement of the encryption scheme.

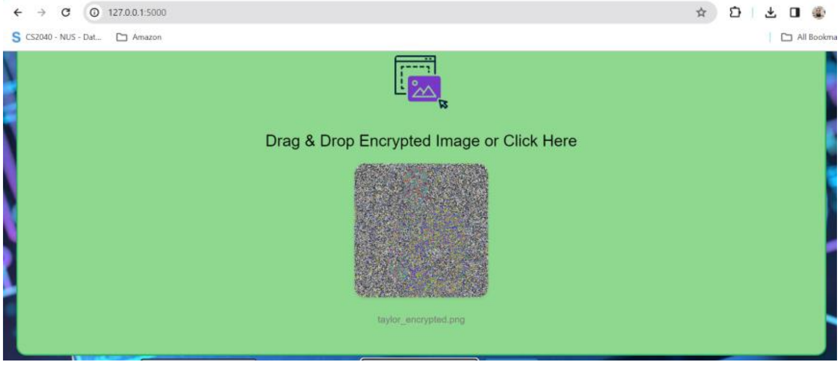
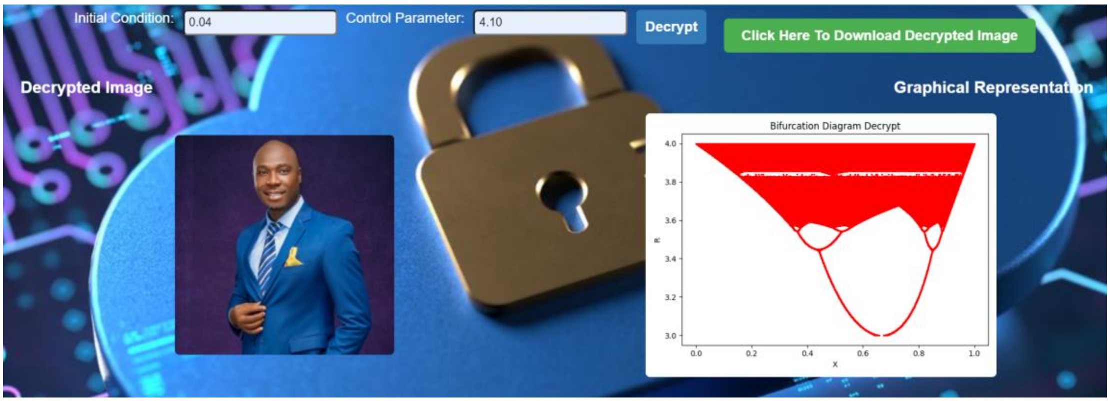


Fig. 12: Encrypted image to be decrypted.



Initial Condition: 0.04

Control Parameter: 4.10

Fig. 13: Decrypted image with Bifurcation diagram

Fig. 13 most likely depicts the visual result of decrypting a picture using a cryptographic algorithm linked to a bifurcation diagram. A bifurcation diagram is a visual depiction that showcases the locations of bifurcation and the patterns of branching within a dynamic system. It is commonly used in encryption methods that rely on chaos. The image shown in Fig. 13 is most likely the outcome of applying the decryption method to an initially encrypted image. The bifurcation diagram may have an impact on the chaotic dynamics that play a role in the decryption process. The interaction between the bifurcation diagram and the decryption algorithm can introduce intricacy and unpredictability, hence bolstering the security and unpredictability of the picture decryption process. The graphic visually represents the decrypted output, highlighting the distinct features generated by the bifurcation diagram during the decryption process of the original image.

5. CONCLUSION

This paper investigates the effectiveness and resilience of encryption algorithms using Histogram Analysis, Adjacent Pixel Autocorrelation Test (APAT), and Key Sensitivity Tests. The proposed method, which combines chaos theory showed promising outcomes in terms of altering spatial relationships between pixels, decreasing information duplication, and guaranteeing responsiveness to significant alterations. The fragility of the Arnold Cat algorithm is a cause for concern. However, the combination of chaos-based encryption algorithms and a customised hash function in a user-friendly web application offers a comprehensive and creative solution to image encryption. The results highlighted the need for achieving a balance between computing efficiency and cryptographic strength. The paper emphasised the need for key sensitivity to ensure security and recommend incorporating image-specific characteristics into hash functions to improve encryption.

6. REFERENCES

[1] M. Mehrtak, S. SeyedAlinaghi, M. MohsseniPour, T. Noori, A. Shamsabadi, M. Heydariet al., "Security challenges and solutions using healthcare cloud computing", Journal of Medicine and Life, vol. 14, no. 4, p. 448-461, 2021. https://doi.org/10.25122/jml-2021-0100

[2] H. Mrabet, S. Belguith, A. Alhomoud, & A. Jemai, "A survey of iot security based on a layered architecture of sensing and data analysis", Sensors, vol. 20, no. 13, p. 3625, 2020. https://doi.org/10.3390/s20133625

[3] M. Eichelberg, K. Kleber, & M. Kämmerer, "Cybersecurity in pacs and medical imaging: an overview", Journal of Digital Imaging, vol. 33, no. 6, p. 1527-1542, 2020. https://doi.org/10.1007/s10278-020-00393-3

[4] R. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (healthchain): evaluation and proof-of-concept study", Journal of Medical Internet Research, vol. 21, no. 8, p. e13592, 2019. https://doi.org/10.2196/13592

[5] S. Liu, X. Liu, J. Yuan, & J. Bao, "Multidimensional information encryption and storage: when the input is light", Research, vol. 2021, 2021. https://doi.org/10.34133/2021/7897849

[6] W. Hong, Z. Yuan, & X. Chen, "Structural color materials for optical anticounterfeiting", Small, vol. 16, no. 16, 2020. https://doi.org/10.1002/smll.201907626

[7] X. Sun, F. Yu, P. Zhang, W. Xie, & X. Peng, "A survey on secure computation based on homomorphic encryption in vehicular ad hoc networks", Sensors, vol. 20, no. 15, p. 4253, 2020. https://doi.org/10.3390/s20154253

[8] M. Bozdal, M. Samie, S. Aslam, & I. Jennions, "Evaluation of can bus security challenges", Sensors, vol. 20, no. 8, p. 2364, 2020. https://doi.org/10.3390/s20082364.

[9] G. Sun, M. Li, J. Zhang, W. Zhang, X. Pei, & Z. Jin, "Transmission dynamics of brucellosis: mathematical modelling and applications in china", Computational and Structural Biotechnology Journal, vol. 18, p. 3843-3860, 2020. https://doi.org/10.1016/j.csbj.2020.11.014

[10] S. Liu, X. Liu, J. Yuan, & J. Bao, "Multidimensional information encryption and storage: when the input is light", Research, vol. 2021, 2021. https://doi.org/10.34133/2021/7897849.

[11] M. Alawida, A. Samsudin, N. Alajarmeh, J. S. Teh, and M. Ahmad, "A novel hash function based on a chaotic sponge and DNA sequence," IEEE Access, vol. 9, pp. 17882-17897, 2021.

[12] I. Aouissaoui, T. Bakir, and A. Sakly, "Robustly correlated key-medical image for DNA-chaos based encryption," IET Image Processing, vol. 15, no. 12, pp. 2770-2786, 2021.

[13] A. A. Bhadke, S. Kannaiyan, and V. Kamble, "Symmetric chaos-based image encryption technique on image bit-planes using SHA-256," in 2018 Twenty Fourth National Conference on Communications (NCC), pp. 1-6, IEEE, February 2018.

[14] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Optics and Lasers in Engineering, vol. 88, pp. 197-213, 2017.

[15] M. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," Optics & Laser Technology, vol. 121, p. 105777, 2020.

[16] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2," Nonlinear Dynamics, vol. 83, pp. 1123-1136, 2016.

[17] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," Symmetry, vol. 12, no. 9, p. 1497, 2020.

[18] H. Liu, A. Kadir, X. Sun, and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and S-boxes," Multimedia Tools and Applications, vol. 77, pp. 1391-1407, 2018.

[19] G. K. Shraida and H. A. Younis, "An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences," Iraqi Journal for Electrical and Electronic Engineering, vol. 18, no. 2, 2022.

[20] X. Zhang, L. Wang, Z. Zhou, and Y. Niu, "A chaos-based image encryption technique utilising Hilbert curves and H-fractals," IEEE Access, vol. 7, pp. 74734-74746, 2019.