International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

A Deep Dive into Chaos-Based Image Encryption - Reviewing, Implementing, and Addressing Challenges

[1]Noor M. Hussein, [2]Nadia M. Mohammed

[1,2]Software Engineering Department, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

Abstract **- Since its introduction in image encryption methods, chaos has proven to be an extremely powerful cryptographic tool. The evolutionary path of chaos-based picture encryption algorithms is thoroughly examined in this article, covering a range of topics including symmetric and asymmetric algorithms, block cyphers, stream cyphers, and their combination with other technologies. The unique properties of chaos, including its pseudo-randomness, topological transitivity, and sensitivity to beginning conditions, make it an ideal subject for interdisciplinary research and provide opportunities to improve image encryption techniques through cross-disciplinary connections. Moreover, the discussion delves into real-world uses, explaining many contexts in which chaotic picture encryption is useful. The thorough examination of chaotic image encryption's current difficulties as well as its useful applications serves as a call to action for researchers. This paper seeks to stimulate further efforts in improving and augmenting the current approaches by providing an overview of the state of the field. Furthermore, it aims to establish a foundation for further developments in chaos-based picture encryption, providing a path for potential growth in this rapidly evolving subject.**

Keywords: Chaos-based Encryption, Encryption Algorithms, Symmetric and Asymmetric Cryptography, Block Ciphers, Stream Ciphers.

I. INTRODUCTION

The deterministic dynamical frameworks that show pseudo-arbitrary and eccentric way of behaving are known as turbulent due to their aversion to starting qualities and boundaries. The investigation of bedlam hypothesis started with H. Poincare's 1913 assessment of the three-body issue. Whenever tumultuous arrangements first got from a deterministic condition in a dissipative framework were seen was in 1963 when E. N. Lorenz presented the Lorenz condition [1]. This was a key moment. Tienyien Li and James A. Yorke formally introduced the term "chaos" in their 1975 publication "Period Three Implies Chaos"[2].

Then, in 1978, M.J. Feigenbaum conducted a thorough analysis of Robert M. May's 1976 Logistic map proposal, which made a significant contribution to the development of chaos theory. Because of its intricacy, sensitivity to beginning circumstances, nonlinearity, and aperiodicity, chaotic systems have become more important in the field of nonlinear dynamics. Applications for chaotic systems' unpredictable character can be found in a wide range of fields [3].

Turbulent frameworks are utilized in money to reenact the mind-boggling conduct of monetary business sectors and give direction to the making of exchanging systems. They support the investigation of populace elements and the way of behaving of natural frameworks in the area of science. Turbulent frameworks are helpful in brain networks for making new calculations for man-made reasoning and AI as well concerning displaying the way of behaving of neurons. Besides, turbulent frameworks have turned into a central part in cryptography, where safe correspondence frameworks are created by using their regular primary likenesses [4].

Robert Matthews's invention of "chaotic encryption" in 1989 was a game-changer, inspiring a plethora of studies on the characteristics of chaotic systems and how orderly systems degenerate into chaotic states. As time has gone on, chaos-based cryptography has developed, going beyond theoretical investigation to real-world implementations, demonstrating the dynamic interplay between chaos theory and actual technical breakthroughs [5].

With the internet's landscape changing so quickly, analyzing and sharing a large number of photographs presents a serious risk to individual privacy. It is now essential to take precautions against the possible leakage of private information. As a result, it is now crucial to put policies in place for image encryption and protection. Specialized structural considerations are required in the field of image encryption due to the unique characteristics of image data, which include strong pixel correlations, enormous capacity, and high redundancy [4].

As a safeguard, image encryption converts picture data into an unintelligible format, guaranteeing the privacy and safety of the content that is displayed. Images are purposefully hidden using encryption algorithms, making it difficult for unauthorized people to understand. Encryption is essential not only for private photos but also for protecting government

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

secrets and trade secrets. Image encryption functions as a barrier to entry in the field of digital image processing, discouraging theft or alteration by unapproved parties [6].

Moreover, image encryption has uses beyond simple confidentiality, such as safeguarding digital watermarks and copyright data. It is crucial to understand, nevertheless, that although picture encryption reduces security risks, it is not impenetrable against hacking or manipulation. Consequently, obtaining complete image security depends critically on the effectiveness and dependability of image encryption techniques [7].

A variety of encryption methods with roots in various technologies have been developed for image encryption in order to achieve this goal. They include DNA-based encryption, optical encryption, S-Box-based encryption, compression encryption, chaos-based encryption, and frequency-domain encryption. The main focus of this study is to explore the nuances of the chaos-based image encryption system, providing insights into its workings and its uses in the larger picture of image security [8].

Traditional encryption algorithms face special issues when dealing with image data due to its strong correlation between neighboring pixels and high redundancy, which naturally require more storage space than text data. These unique features make conventional methods difficult to suit the specific requirements of image encryption. Nevertheless, a viable approach presents itself when chaos theory is incorporated into picture encryption, providing a fresh and efficient fix [9].

According to a paradigm introduced by chaos theory, chaotic systems are very sensitive to initial conditions and can display drastically diverse motion trajectories even with small initial setup faults [10]. In any event, when tumultuous directions are deterministically constrained through determined starting conditions, the drawn-out forecast of these directions is generally eccentric without any definite information on the underlying setup. Turbulent frameworks additionally have other significant qualities that are helpful in the field of picture encryption, like high ergodicity, assurance, and pseudo-irregularity [11].

This paper investigates Chaos-Based Image Encryption in great detail. It covers important topics including an overview of the subject, a detailed analysis of chaotic systems, an investigation of the RC4 Key Generation Algorithm, a comprehensive review of the literature, and a look at the difficulties that arise with Chaos-Based Image Encryption. The study wraps off with a summary of its discoveries and learnings. The writers present a comprehensive analysis of the topic throughout the paper, fusing theoretical debates with real-world applications. A literature review adds dimension to the paper and provides readers with a thorough grasp of the state of the field's research. The difficulties section clarifies possible obstacles to Chaos-Based Image Encryption implementation, offering insightful information for further study and improvement.

II. CHAOTIC SYSTEMS

Chaos systems can be divided into two categories based on how they change over time: discrete chaotic maps and continuous chaotic systems [12]. Within the domain of continuous chaotic systems, a system of differential equations controls the state's continuous evolution throughout time. Conversely, discrete chaotic maps show systems in which the state follows usually iterative equations and changes discretely over time.

A turbulent guide is a numerical capability that shows tumultuous way of behaving when iterated over the long run. Turbulent way of behaving, in this specific circumstance, alludes to a framework that is profoundly delicate to starting circumstances, shows aperiodic and flighty directions, and displays a specific level of haphazardness. Tumultuous guides have tracked down applications in different logical and designing fields, including cryptography, picture handling, and arbitrary number age [13]. Table (1) shows chaotic maps.

Table 1: Chaotic Maps

Chaotic Map	Description	Equations
Logistic Map [14]	Famous for its various behaviors, including periodic, bifurcations, and chaos.	$x_{n+1} = r.x_n(1 - x_n)$
Henon Map [15]	Commonly used in image encryption, known for its sensitivity to initial conditions.	$x_{n+1} = 1 - a.x_n^2 + y_n$ $y_{n+1} = b.x_n$
Tent Map [16]	Exhibits a tent-like shape and is often used in random number generation.	$x_{n+1} = r.x_n \; for \; 0 \leq x_n \leq 0.5$ $x_{n+1} = r(1 - x_n) for \; 0.5 \leq x_n \leq 1$
Lorenz System [17]	Represents a simplified model of atmospheric convection, known for its "butterfly" attractor.	$\frac{dx}{dt} = \sigma.(y - x)$

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 12, pp 271-280, December-2023

https://doi.org/10.47001/IRJIET/2023.712037

		$\frac{dy}{dt} = \sigma.(\rho - x) - y$ $\frac{dz}{dt} = x.y - \beta.z$
Rossler System [18]	Used in studying chaotic oscillations in chemical reactions and fluid dynamics.	$\frac{dx}{dt} = -x - y$ $\frac{dy}{dt} = x + a.y$ $\frac{dz}{dt} = b + z.(x - c)$
Arnold's Cat Map [19]	Commonly used in image scrambling and encryption due to its mixing properties.	$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} . \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ M$

These chaotic maps have diverse applications in fields such as cryptography, secure communications, random number generation, and modeling complex systems. The choice of a specific chaotic map depends on the requirements of the application and the desired properties of the chaotic behavior [20].

III. RC4 KEY GENERATION ALGORITHM

The RC4 key age calculation, a vital part of the RC4 stream figure created by Ron Rivest, organizes an enamoring pseudorandom dance. The calculation works on a 8×8 S-box, indicated as S0, S1,..., S255, where every passage is a change of the numbers 0 through 255. The actual stage is complicatedly attached to the variable-length key, giving a unique establishment to the cryptographic cycle [21]. RC4 utilizes two counters, I and j, both introduced to nothing, as it leaves on the excursion of producing a pseudorandom byte. The cycle unfurls through a painstakingly created dance of these counters, rearranging and trading components inside the S-box. The outcome is a hypnotizing exchange of cryptographic complexities, delivering a flood of pseudorandom bytes that are then XORed with the information stream. This ensemble of tasks exemplifies the embodiment of RC4, a flexible variable-key-size stream figure that has made a permanent imprint on the scene of cryptographic calculations [22].

The heart of the RC4 encryption and decryption processes lies in the elegant simplicity of bitwise XOR operations. In the encryption phase, the ciphertext emerges by XORing each byte of the plaintext with the corresponding byte from the pseudorandom stream generated by the RC4 algorithm. This bitwise operation, byte by byte, ensures a secure transformation of the original data. The decryption process mirrors this elegance, with the plaintext being faithfully re-produced by XORing the ciphertext with the same byte stream, ensuring the reversibility of the cryptographic operation. This symmetry underscores the fundamental concept of symmetric key cryptography, where the same key is used for both encryption and decryption. For a deeper exploration of RC4 and its intricacies, one can refer to the comprehensive insights provided in the cited sources [23]. Figure (1) summarize RC4 processing flowchart.

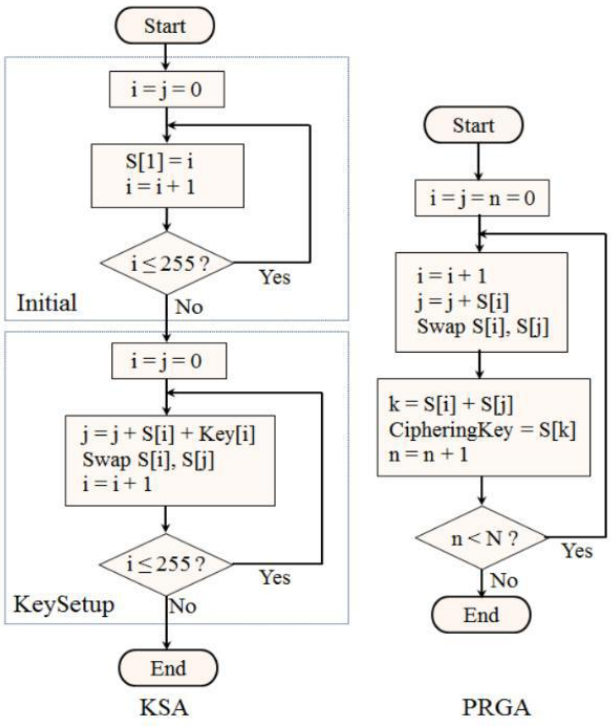

Figure 1: RC4 processing flowchart [24]

IV. LITERATURE SURVEY

A detailed summary of the several images and multimedia encryption techniques put forth by various researchers is given in the table (2). The goal of these encryption methods is to improve multimedia and digital picture security and confidentiality. In order to protect sensitive data in a variety of applications, from general image encryption to specialized use cases like medical image protection and secure communication in cutting-edge technologies like 6G networks and IoT, the techniques cover a

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

broad range of chaotic systems, cryptographic algorithms, and creative approaches.

To add complexity and randomness to the encryption processes, researchers have looked into a variety of chaotic systems, including hyperchaotic systems, Baker maps, Chen's chaotic systems, and logistic maps. Furthermore, several encryption schemes have included cryptographic algorithms like RSA and DNA-based techniques, demonstrating the flexibility of fusing traditional and modern technologies for strong security.

The table also discusses developments in embedded systems, such as microcontrollers, and offers solutions for problems with implementation, processing resources, and finite accuracy. The incorporation of chaotic encryption algorithms into these systems illustrates how the suggested techniques can be used in real-world situations.

The presented research contributions also extend to the field of medical image encryption, introducing schemes that leverage DNA technology, adaptive tracking mechanisms, and neural networks to secure sensitive medical data. The exploration of color image encryption, cross-plane permutation, and compound chaotic maps illustrates the efforts to address specific challenges associated with multimedia data.

Table 2: Related Works Survey

Authors	Proposed Method/Algorithm	Key Contributions
Lian and Sun [25]	2D Standard Guide, Strategic Guide, and Tent Guide Based Encryption	Used a 2D Standard guide for disarray, Strategic guide for dispersion, and Tent guide for key age. Presented a dissemination impact in the replacement stage to upgrade encryption time.
Guan [26]	3D Chen's Tumultuous Framework Based Picture Encryption	Presented a 3D Chen's tumultuous framework-based picture encryption strategy, XORing successions from Chen's framework with various sub-blocks of the first picture.
Xiang and Liao [27]	Calculated Guide Based Picture Encryption with Key-Subordinate Shift Approach	Presented a Strategic guide-based picture encryption utilizing key-subordinate shift approach and stage dispersion-based method.
Pareek and Patidar [28]	Picture Encryption In light of Calculated Guides	Utilized two Strategic guides, with the first creating starting circumstances for the second. Utilized an outside 80-bit secret key and different tasks to scramble picture pixels. Unscrambling tasks were determined by the Calculated guide end results.
Xiao and Liao [29]	Examination and Improvement of Guan's Picture Encryption	Examined defects in Guan's strategy and further developed it, resolving issues connected with the quantity of rounds, keystream intricacy, and fastening relations.
Tong and Cui [30]	Compound Two-Layered Tumultuous Guide with 3D Dough puncher Guide	Proposed a compound two-layered turbulent guide for tumultuous grouping age. Utilized two one-layered turbulent guides that switch haphazardly. Encoded the picture with a 3D Cook guide to address accuracy limits of one-layered turbulent capabilities.
Amin and Faragallah[31]	Picture Encryption In light of Crude Activities and Tent Guide	Introduced a picture encryption technique utilizing crude tasks, nonlinear changes, and a tumultuous Tent guide. Cryptographic tasks depended on piece obstructs instead of pixel blocks. Involved 256-cycle meeting keys for encryption.
Wang and Wong [32]	Closest Neighbor Coupled-Guide Grids (NCMLs) Picture Encryption	Presented NCMLs, producing a pseudo-irregular succession. Utilized a S-Box of AES and a 128-bit outer key to reset pixel esteems and migrate picture blocks.
Huang [33]	Boundary Improved Two-Layered Cross-Tumultuous Chebyshev Framework	Added boundaries to a two-layered cross-turbulent Chebyshev framework to improve responsiveness and key space. Created a pseudo-irregular tumultuous succession for disarray and dispersion.
Mihai Stanciu and Octaviana Datcu [34]	Tumultuous Encryption Calculation Executed on Atmel AVR Microcontroller	Proposed a tumultuous encryption calculation carried out on an Atmel AVR microcontroller in 2012. Zeroed in on the implanted framework industry, explicitly microcontrollers, giving an underlying execution yet needed itemized security execution examination.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 12, pp 271-280, December-2023

https://doi.org/10.47001/IRJIET/2023.712037

Nooshin Bigdeli and Yousef Farid [35]	Picture Encryption with Tumultuous Neuron Layer (CNL) and Change Neuron Layer (PNL)	Proposed picture encryption in light of a turbulent neuron layer (CNL) and a change neuron layer (PNL). Utilized a three-input (RGB worth) and three-yield (encoded streams) CNN structure. Used three turbulent frameworks to create the loads and inclinations grids of the CNL. Accomplished 3D stage through rounds of change with straight stage and 2D nonlinear rearranging.
Fouda and Effa [36]	PWLCM-Based Tumultuous Picture Encryption with Straight Diophantine Condition	Proposed a PWLCM-based turbulent picture encryption strategy using the Straight Diophantine Condition (LDE). LDE includesیindispensable coefficients for at least one factors, guaranteeing arrangements are whole numbers.
Sui and Duan [37]	Deviated Twofold Picture Encryption with Fragmentary Change and Turbulent Strategic Guide	Presented awry twofold (different) picture encryptions. One including Fourier change, while the other related with discrete fragmentary irregular change.
Ahmed and Xiamu Niu [38]	Picture Encryption Hybridizing Cyclic Elliptic Bend and Tumultuous Framework	Hybridized a cyclic elliptic bend and a tumultuous framework to plan quicker and safer picture encryptions. Roused further examination thoughtfulness regarding elliptic bends in turbulent picture encryption.
Wang and Liu [39]	Dynamic Arbitrary Development Method in Feline Guide Based Encryption	Presented dynamic irregular development procedure in a Feline guide-based picture encryption strategy to improve security. Tended to holes in customary stage processes making the encryption safer against assaults.
Liu and Kadir [40]	Deviated Encryption Utilizing Hash-512 and Complex Turbulent Framework	Utilized Hash-512 inside the plain picture to start values. Incorporated a four-wing complex turbulent framework for deviated picture encryption. Consecutively preprocessed parts in red, yellow, and blue involving a turbulent succession for encryption.
Chen and Zhu [41]	Dynamic State Factors Choice Component (DSVSM)	Proposed a DSVSM-based picture encryption calculation utilizing a Chen map. Developed the calculation to address imperfections in four ways, upgrading its general security.
Liu and Miao [42]	Calculated Guide Based Encryption with Differing Boundaries	Introduced a Strategic guide based picture encryption strategy with differing boundaries. Further developed power against stage space recreation assaults by permitting boundaries to haphazardly change.
M. A. Murilo-Escobar and C. Cruz-Hernandez [43]	Further developed Turbulent Encryption Calculation on Implanted 32-cycle Microcontroller	Given an upgraded tumultuous encryption calculation superior execution and low execution required assets. Executed on an implanted 32-digit microcontroller, resolving issues of low chip memory, low recurrence and speed, and the shortfall of a parallelism structure in their plan.
Pak and Huang [44]	Tumultuous Framework Mix for Direct Nonlinear-Straight Change	Utilized two of the three 1D tumultuous guides to build another turbulent framework for encryption. Further developed the direct nonlinear construction based turbulent picture encryption to a straight nonlinear-direct transformation structure. Upgraded tumult by joining maps with high data entropy and a Lyapunov type.
Wu and Xiaofeng [45]	Deviated Picture Encryption with Elliptic Bend and Turbulent Framework	Presented an awry picture encryption technique consolidating an elliptic bend (EC) and tumultuous framework. Utilized a 4D Feline guide and 3D Lorenz condition for change and dissemination. Empowered transmission of private data with little key gatherings and numbers.
Ünal and Akif [46]	Cross breed RSA Encryption Calculation with Turbulent RNG	Planned a cross breed RSA (CRSA) encryption calculation with a tumultuous RNG. Incorporated the circuit acknowledgment of a turbulent framework. Joined benefits of RSA and tumultuous frameworks.
K. Ratnavelu and M. Kalpana	Picture Encryption with Fluffy Cell Brain Organization	Presented a fluffy cell brain organization (FCNN) for picture encryption. Distinguished the worth of FCNN boundaries to create

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

[47]	(FCNN)	tumultuous arrangements for picture encryption.
Wang and Wang [48]	Deviated Picture Encryption with Round and hollow Diffraction Irregular Stage Encoding and Reservation-Truncation	Introduced an awry picture encryption calculation utilizing round and hollow diffraction arbitrary stage encoding (DCRE) and reservation-truncation (PRT). DCRE encoded the plain picture, and PRT isolated the diffraction dispersion into stage and sufficiency, filling in as uneven keys.
Siva Janakiraman and K Thenmozhi [49]	Lossless Picture Encryption Calculation with Reversible Lightweight Activities	Proposed a lossless picture encryption calculation utilizing reversible lightweight tasks. The turbulent key was created by a solitary accuracy drifting point microcontroller, tending to the lack of on-chip memory accessible for microcontrollers.
Dolendro and Manglem[50]	Tumult Based Picture Encryption with Diffie-Hellman Key Trade	Introduced a bedlam based picture encryption strategy using the Diffie-Hellman key trade procedure. Keys are produced in the wake of sharing an irregular point on an elliptic bend.
Nardoa and Nepomuceno [51]	Picture Encryption Utilizing Tumultuous Framework with Limited Precision Mistake	Utilized limited precision blunder as a wellspring of haphazardness in picture encryption. Utilized the Chua framework and a variable in view of the plain picture to create keystream. Resolved the issue of turbulent framework corruption because of restricted PC exactness.
Akram Belazi and Muhammad Talha [52]	Clinical Picture Encryption Plan with DNA Innovation, Hash Capability, and Tumultuous Frameworks	Joined DNA innovation, a hash capability, and tumultuous frameworks to devise a clinical picture encryption conspire.
Xing-Yuan Wang and Zhi-Ming Li [53]	Picture Encryption with Hopfield-CNN and Tumultuous Guides	Presented a Hopfield-CNN-based picture encryption approach. Used tumultuous guides, including the Feline guide and staged composite turbulent guide, for disarray in the picture encryption stage. Applied Hopfield CNN in the dispersion step.
Liping Chen and Hao Yin [54]	Picture Encryption with 3D Fragmentary Request Discrete Hopfield Brain Organization (FODHNN)	Built a 3D partial request (FO) discrete Hopfield brain organization (FODHNN) with tumultuous elements highlights. Utilized the FODHNN as a PRNG in picture encryption.
Hua and Zhu [55]	2D Calculated Tent Secluded Guide (2D-LTMM) for Variety Picture Encryption	Developed a 2D Strategic Tent secluded map (2D-LTMM) to beat deficiencies. Introduced a variety picture encryption calculation utilizing cross-plane change and non-successive dispersion to simultaneously scramble the three variety planes of pictures.
Shakiba [56]	Chebyshev Polynomial-Based Picture Encryption with Turbulent PRNG	Proposed a Chebyshev polynomial-based picture encryption calculation using a turbulent PRNG for repeating a one-time cushion. Altogether extended the critical space and upgraded protection from picked plaintext assaults (CPA).
Behrouz and Saleh [57]	Versatile Terminal Sliding Mode Following for Synchronization in Clinical Picture Encryption	Presented a versatile terminal sliding mode following methodology for synchronization among shipper and recipient in clinical picture encryption. Used synchronized turbulent frameworks to improve the security of picture transmission or capacity.
Zhang and Zhang [58]	Deviated Picture Encryption with Hyperchaotic Framework, DNA Activity, Feline Guide, and Stage Shortened Fragmentary Fourier Change	Endeavored a mix of strategies in uneven picture encryption, including a hyperchaotic framework, DNA-level activity, Feline guide, and stage shortened fragmentary Fourier change (ptFrFT). Shown solid protection from the two-step iterative adequacy stage recovery calculation.
Ye and Wu [59]	Deviated Picture Encryption with 3D ILM Turbulent Framework and RSA	Presented a 3D ILM turbulent framework with a huge key space and high intricacy. Made a numerical model of key procurement (MKA). Consolidated the new framework with RSA for hilter kilter picture encryption.

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

V. THE CHALLENGES OF CHAOS-BASED IMAGE ENCRYPTION

Looking at the ongoing difficulties in confusion-based picture encryption is urgent for improving its general viability and moderating possible weaknesses. The ID of these difficulties fills in as an impetus for scientists to acquire new bits of knowledge and motivation in creating novel encryption procedures that proposition uplifted security, proficiency, and ease of use. These difficulties, saw as any open doors for additional innovative work, basically spin around two key angles: protection from cryptanalysis or assault and the handling of encoded pictures [60].

The evolving landscape of chaos-based image encryption technology, while making strides in security and robustness, is not without vulnerabilities. Notably, the resistance to attacks remains a paramount concern, with scholarly investigations revealing vulnerabilities in existing schemes. The need to fortify image-encryption algorithms against chosen-plaintext and chosen-ciphertext attacks underscores the ongoing quest for more secure implementations. Another significant challenge lies in the processing of encrypted images, particularly in the domains of image compression and retrieval [61].

VI. CONCLUSION

In terms of image security, chaos-based image encryption is still very successful. In order to provide insights into the evolution of chaos-based picture encryption, this work undertakes a thorough overview and analysis of symmetric and asymmetric encryption techniques. For a thorough knowledge of the evolution of image-encryption algorithms, a comprehensive timeline and performance evaluation are provided. Furthermore, the research explores the incorporation of chaotic systems with various technologies in image encryption, such as cellular automata, blockchain, elliptic curve, neural networks, genetic algorithms, and DNA technology. Its unique properties, including its sensitivity to beginning conditions, topological transitivity, and ability to generate pseudo-random sequences, encourage multidisciplinary cooperation and ongoing improvements in image-encryption techniques.

Moreover, the significance of chaos-based picture encryption in real-world uses is emphasized. The study describes particular applications of this technology in the microcontroller area, Internet of Things (IoT), medical field, and satellite applications. Chaos-based picture encryption has advantages, but it also has disadvantages. The work specifically covers two important issues: the complexity of processing encrypted images and the requirement for strong resistance against cryptanalysis or attacks. These difficulties, nevertheless, are more than just roadblocks; they also offer chances for more research and development, acting as spurs for subsequent breakthroughs in chaotic picture encryption techniques.

In summary, this study highlights the potential of chaos-based picture encryption and stresses the necessity of continuous research and development to improve its security, effectiveness, and usability, all the while admitting the current obstacles. The objective is to guarantee the secure and private handling of sensitive data in the dynamic digital environment by tackling existing issues and investigating novel approaches.

ACKNOWLEDGEMENT

Authors would like to thank Mosul University for support.

REFERENCES

[1] E. N. (M. I. T. . Lorenz, "Lorenz_Deterministic_Nonperiodic_Flow_1962.Pdf," *Journal of the Atmospheric Sciences*, vol. 20. p. 12, 1962.

[2] T.-Y. Li and J. A. Yorke, "Period Three Implies Chaos BT - The Theory of Chaotic Attractors," B. R. Hunt, T.-Y. Li, J. A. Kennedy, and H. E. Nusse, Eds., New York, NY: Springer New York, 2004, pp. 77–84. doi: 10.1007/978-0-387-21830-4_6.

[3] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976, doi: 10.1038/261459a0.

[4] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol. 27, no. 4, pp. 623–656, 1948, doi: 10.1002/j.1538-7305.1948.tb00917.x.

[5] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976, doi: 10.1038/261459a0.

[6] M. Maqableh, "A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map," *J. Softw. Eng. Appl.*, vol. 08, no. 12, pp. 635–659, 2015, doi: 10.4236/jsea.2015.812059.

[7] M. Sobhy and R. Alaa, *Chaotic algorithms for data encryption*, vol. 2. 2001. doi: 10.1109/ICASSP.2001.941085.

[8] X. Zhang and W. Chen, *A new chaotic algorithm for image encryption*. 2008. doi: 10.1109/ICALIP.2008.4590187.

[9] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11. 2023. doi: 10.3390/math11112585.

[10] G. Tang, S. Wang, H. Lü, and G. Hu, "Chaos-based cryptograph incorporated with S-box algebraic operation," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 318, no. 4–5, pp. 388–398, 2003, doi: 10.1016/j.physleta.2003.09.042.

[11] G. Tang, S. Wang, H. Lü, and H. Gang, "Chaos-based cryptograph incorporated with S-box algebraic

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

operation," *Phys. Lett. A*, vol. 318, pp. 388–398, Nov. 2003, doi: 10.1016/j.physleta.2003.09.042.

[12] T. Azizi and B. Alali, "Chaos Induced by Snap-Back Repeller in a Two Species Competitive Model," *Am. J. Comput. Math.*, vol. 10, no. 02, pp. 311–328, 2020, doi: 10.4236/ajcm.2020.102017.

[13] H. A. J. Al-Asady, O. Q. J. Al-Thahab, and S. S. Hreshee, "Robust Encryption System Based Watermarking Theory by Using Chaotic Algorithms: A Reviewer Paper," *J. Phys. Conf. Ser.*, vol. 1818, no. 1, 2021, doi: 10.1088/1742-6596/1818/1/012086.

[14] Ł. Pawela and K. Życzkowski, "Matrix logistic map: fractal spectral distributions and transfer of chaos," *arXiv:2303.06176v1*, pp. 1–8, 2023, [Online]. Available: http://arxiv.org/abs/2303.06176

[15] F. Bianchi and T.-C. Dinh, "Every complex H{\'e}non map is exponentially mixing of all orders and satisfies the CLT," vol. 80, pp. 1–11, 2023, [Online]. Available: http://arxiv.org/abs/2301.13535

[16] K. Scheicher, V. F. Sirvent, and P. Surer, "Dynamical properties of the tent map," *J. London Math. Soc.*, vol. 93, no. 2, pp. 319–340, 2016, doi: 10.1112/jlms/jdv071.

[17] S. F. Al-Azzawi, Mujiarto, L. Patria, A. Sambas, and W. S. M. Sanjaya, "Stability of Lorenz System at the Second Equilibria Point based on Gardano's Method," *J. Phys. Conf. Ser.*, vol. 1477, no. 2, 2020, doi: 10.1088/1742-6596/1477/2/022009.

[18] A. Kumar, "Rossler's system using piecewise derivative," *Results Phys.*, vol. 50, no. March, p. 106555, 2023, doi: 10.1016/j.rinp.2023.106555.

[19] J. Bao and Q. Yang, "Period of the discrete Arnold cat map and general cat map," *Nonlinear Dyn.*, vol. 70, no. 2, pp. 1365–1375, 2012, doi: 10.1007/s11071-012-0539-3.

[20] M. Lawnik and M. Berezowski, "New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography," *Symmetry (Basel).*, vol. 14, no. 5, 2022, doi: 10.3390/sym14050895.

[21] M. H. S. Hasan, "Image Encryption using Modified RC4 Algorithm," in *2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 2023, pp. 430–434. doi: 10.1109/MI-STA57575.2023.10169339.

[22] S. Sriadhi, R. Rahim, and A. S. Ahmar, "RC4 Algorithm Visualization for Cryptography Education," *J. Phys. Conf. Ser.*, vol. 1028, no. 1, 2018, doi: 10.1088/1742-6596/1028/1/012057.

[23] S. Kareem, "Image Encryption by Using RC4 Algorithm Image Encryption by Using RC4 Algorithm," *Eur. Acad. Res.*, no. July 2014, 2014.

[24] T. H. Tran, L. Lanante, Y. Nagao, M. Kurosaki, and H. Ochi, "Hardware Implementation of High Throughput RC4 algorithm," *ISCAS 2012 - 2012 IEEE Int. Symp. Circuits Syst.*, no. June 2014, pp. 77–80, 2012, doi: 10.1109/ISCAS.2012.6272151.

[25] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, 2005, doi: https://doi.org/10.1016/j.chaos.2004.11.096.

[26] Z. H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 346, no. 1–3, pp. 153–157, 2005, doi: 10.1016/j.physleta.2005.08.006.

[27] T. Xiang, X. Liao, G. Tang, Y. Chen, and K. Wong, "A novel cryptosystem based on iterating a chaotic map," *Phys. Lett. A*, vol. 349, pp. 109–115, Jan. 2006, doi: 10.1016/j.physleta.2005.02.083.

[28] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006, doi: https://doi.org/10.1016/j.imavis.2006.02.021.

[29] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009, doi: https://doi.org/10.1016/j.chaos.2007.10.009.

[30] X. Tong and M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," *Signal Processing*, vol. 89, no. 4, pp. 480–491, 2009, doi: https://doi.org/10.1016/j.sigpro.2008.09.011.

[31] M. Amin, O. Faragallah, and A. Abd El-Latif, "A chaotic block cipher algorithm for image cryptosystems," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, pp. 3484–3497, Nov. 2010, doi: 10.1016/j.cnsns.2009.12.025.

[32] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011, doi: https://doi.org/10.1016/j.asoc.2009.12.011.

[33] X. Huang, "Image encryption algorithm using chaotic Chebyshev generator," *Nonlinear Dyn.*, vol. 67, no. 4, pp. 2411–2417, 2012, doi: 10.1007/s11071-011-0155-7.

[34] M. Stanciu and O. Datcu, *Atmel AVR microcontroller implementation of a new enciphering algorithm based on a chaotic Generalized Hénon Map*. 2012. doi: 10.1109/ICComm.2012.6262554.

[35] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, 2012, doi: https://doi.org/10.1016/j.engappai.2012.01.007.

[36] J. S. Armand Eyebe Fouda, J. Yves Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 3, pp. 578–588, 2014, doi: https://doi.org/10.1016/j.cnsns.2013.07.016.

[37] L. Sui, K. Duan, J. Liang, and X. Hei, "Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps," *Opt. Express*, vol. 22, no. 9, p. 10605, 2014, doi: 10.1364/oe.22.010605.

[38] A. A. A. El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimed. Tools Appl.*, vol. 70, no. 3, pp. 1559–1584, 2014, doi: 10.1007/s11042-012-1173-2.

[39] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 271-280, December-2023
https://doi.org/10.47001/IRJIET/2023.712037

image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, 2015, doi: https://doi.org/10.1016/j.optlaseng.2014.08.005.

[40] H. Liu, A. Kadir, and Y. Li, "Asymmetric color pathological image encryption scheme based on complex hyper chaotic system," *Optik (Stuttg).*, vol. 127, no. 15, pp. 5812–5819, 2016, doi: https://doi.org/10.1016/j.ijleo.2016.04.014.

[41] J. Chen, Z. Zhu, C. Fu, H. Yu, and L. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 3, pp. 846–860, 2015, doi: https://doi.org/10.1016/j.cnsns.2014.06.032.

[42] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *Springerplus*, vol. 5, no. 1, p. 289, 2016, doi: 10.1186/s40064-016-1959-1.

[43] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. López-Gutiérrez, "Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller," *Microprocess. Microsyst.*, vol. 45, pp. 297–309, 2016, doi: https://doi.org/10.1016/j.micpro.2016.06.004.

[44] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017, doi: https://doi.org/10.1016/j.sigpro.2017.03.011.

[45] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, 2017, doi: https://doi.org/10.1016/j.optlaseng.2016.10.019.

[46] Ü. Çavuşoğlu, A. Akgül, A. Zengin, and I. Pehlivan, "The design and implementation of hybrid RSA algorithm using a novel chaos based RNG," *Chaos, Solitons & Fractals*, vol. 104, pp. 655–667, 2017, doi: https://doi.org/10.1016/j.chaos.2017.09.025.

[47] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, and P. Raveendran, "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Processing*, vol. 140, pp. 87–96, 2017, doi: https://doi.org/10.1016/j.sigpro.2017.05.002.

[48] J. Wang, Q. H. Wang, and Y. Hu, "Asymmetric Color Image Cryptosystem Using Detour Cylindrical-Diffraction and Phase Reservation Truncation," *IEEE Access*, vol. 6, pp. 53976–53983, 2018, doi: 10.1109/ACCESS.2018.2871102.

[49] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller," *Microprocess. Microsyst.*, vol. 56, pp. 1–12, 2018, doi: https://doi.org/10.1016/j.micpro.2017.10.013.

[50] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimed. Tools Appl.*, vol. 77, no. 7, pp. 8629–8652, 2018, doi: 10.1007/s11042-017-4755-1.

[51] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov, "Image encryption using finite-precision error," *Chaos, Solitons & Fractals*, vol. 123, pp. 69–78, 2019, doi: https://doi.org/10.1016/j.chaos.2019.03.026.

[52] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[53] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, 2019, doi: https://doi.org/10.1016/j.optlaseng.2018.11.010.

[54] L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," *Neural Networks*, vol. 125, pp. 174–184, 2020, doi: https://doi.org/10.1016/j.neunet.2020.02.008.

[55] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Inf. Sci. (Ny).*, vol. 546, pp. 1063–1083, 2021, doi: https://doi.org/10.1016/j.ins.2020.09.032.

[56] A. Shakiba, "A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 5, pp. 562–571, 2021, doi: https://doi.org/10.1016/j.jksuci.2019.03.003.

[57] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast Reaching Finite Time synchronization Approach for Chaotic Systems With Application in Medical Image Encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021, doi: 10.1109/ACCESS.2021.3056037.

[58] Y. Zhang, L. Zhang, Z. Zhong, L. Yu, M. Shan, and Y. Zhao, "Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation," *Opt. Lasers Eng.*, vol. 143, p. 106626, 2021, doi: https://doi.org/10.1016/j.optlaseng.2021.106626.

[59] G.-D. Ye, H.-S. Wu, X.-L. Huang, and S.-Y. Tan, "Asymmetric image encryption algorithm based on a new three-dimensional improved logistic chaotic map," *Chinese Phys. B*, vol. 32, no. 3, p. 30504, 2023, doi: 10.1088/1674-1056/ac7dbb.

[60] C. Yang, P. Pan, and Q. Ding, "Image Encryption Scheme Based on Mixed Chaotic Bernoulli Measurement Matrix Block Compressive Sensing," *Entropy*, vol. 24, no. 2. 2022. doi: 10.3390/e24020273.

[61] W. Song, C. Fu, Y. Zheng, L. Cao, M. Tie, and C.-W. Sham, "Protection of image ROI using chaos-based encryption and DCNN-based object detection," *Neural Comput. Appl.*, vol. 34, no. 7, pp. 5743–5756, 2022, doi: 10.1007/s00521-021-06725-w.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 12, pp 271-280, December-2023

https://doi.org/10.47001/IRJIET/2023.712037

Citation of this Article:

Noor M. Hussein, Nadia M. Mohammed, "A Deep Dive into Chaos-Based Image Encryption - Reviewing, Implementing, and Addressing Challenges" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 12, pp 271-280, December 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.712037

****

