Volume 9, Issue 7, July – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1510

Computational Competent & Random Key based Image Cryptography for Dynamic Network: A Literatutre Review

Jashwant Samar
Research Scholar, Computer Science and Engineering
Rabindranath Tagore University (RNTU)
Raisen, India

Shailja Sharma
Associate Professor,
Computer Science and Engineering
Rabindranath Tagore University (RNTU)
Raisen, India

Ankur Khare
Assistant Professor,
Computer Science and Information Technology
Rabindranath Tagore University (RNTU)
Raisen, India

Abstract:- The rising abundance of vibrant networks, like Mobile Ad-hoc Networks (MANETs), Wireless Sensor Networks (WSNs), and Flying Ad-hoc Networks (FANETs) requires sophisticated cryptographic solutions to protect multimedia information delivery. This paper offers a thorough review of computationally competent and random key-based image cryptography adapted for vibrant network circumstances. We search the background of image cryptography alongside an emphasis on algorithms and strategies that highlight computational competence and the utilization of random keys for improved protection. Key ranges enclosed comprise conventional symmetric and asymmetric encryption schemes, trivial cryptography, and logistic system related key production schemes. The paper explores the capabilities and restraints of these schemes based on encryption time, key administration and protection strength. An exhaustive examination of several random key production schemes is offered, exhibiting how these schemes cause to enhance randomness and vigour in cryptography. We deliberate the incorporation of these schemes in vibrant networks where systems frequently tackle restrictions such as rare processing energy, storage and power. The paper also discusses the issues impersonated through such circumstances, containing the requirement for real-time information processing, flexibility and compliance to modify network situations. The paper calculates the strength of latest techniques utilizing performance vectors like encryption speed, key sensibility and resilience to cryptanalysis attacks.

Keywords:- *Cryptographic, Vibrant Network, Symmetric, Asymmetric, Encryption Time.*

I. INTRODUCTION

In tech epoch, protecting multimedia information, particularly images, has developed vital because of the broad utilization of vibrant networks [1]. The vibrant networks are illustrated through their vibrant topologies, restricted resources, and the subsequent requirement for real-time information delivery. This circumstance forces distinctive issues for encryption methods, requiring solutions that are protected and computationally competence. Conventional encryption methods, while vigorous, frequently fall concise in vibrant network surroundings because of their maximum computational overhead and key controlling intricacy. So, there is an imperative requirement for encryption mechanism that can equalize the adjustment between protection and competence [5, 15]. This equalization is essential for resource inhibited systems that must accomplish encryption processes quickly devoid of using their restricted computational strength. A capable scheme to discourse these issues is development of image encryption schemes that deploy random key creation. Random keys add volatility in cryptographic operation, building it considerably tough for intruders to interrupt the encryption by brute force, cryptanalysis attacks and statistical attacks. Furthermore, incorporating trivial encryption approaches certifies that these mechanisms can utilize essentially within the rigorous resource restrictions of vibrant networks [3].

This review paper offers a thorough summary of state-of-the-art in computationally competent and random key based image cryptography [4, 7]. The main aim is on finding the higher competent schemes and systems that utilize with the requirements of vibrant networks. Additionally, this paper illustrates the practical development issues and safety consequences of implementing these mechanisms in vibrant network circumstances. By examining latest trends and contemporary improvements, the review focusses gaps in latest research and offers routes for future implements in acute epoch of encryption. The crucial objective is to adopt innovations that improve protection while managing computational

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1510

competence, certifying the consistent safety of multimedia information in gradually interrelated [10].

II. LITERATURE REVIEW

The era of image encryption in vibrant network has been expressive progressions, determined through the demand to protect multimedia information in circumstances considered by inconsistent connectivity and inhibited resources. This survey illustrates the major developments and strategies that have appeared, highlighting computational strength and arbitrary key production [6, 8].

A. Symmetric Cryptography

Symmetric cryptographic strategies, like Advanced Encryption Standard (AES), are broadly utilized for their rapidity and easiness. AES is especially famous for its tough protection and effectiveness, building it a wide spread selection for encrypting images in vibrant network. Many researchers proposed several modified AES schemes adapted for IoT systems that diminishes the computational overhead while managing cryptographic efficiency [14].

Regardless of their benefits, these strategies encounter issues in key management. The requirement to safe dispersion and manage keys in vibrant networks with numerous topology modifications can be complicated and susceptible to attacks [3]. To tackle this, numerous research works have illustrated hybrid systems merging the symmetric cryptographic strategies with dynamic key production to improve the protection devoid of compromising effectiveness.

B. Asymmetric Encryption

Asymmetric cryptographic strategies, like Elliptic Curve Cryptography (ECC) [12], are vital for safe key interchange and digital signatures in vibrant network. ECC is specifically beneficial because of its minimum key size, offering tough protection with minimum computational load. Several research works illustrated an ECC related image cryptographic system that successfully equivalence protection and computational competence for mobile network.

Yet, the computational power of asymmetric strategies frequently boundaries their open application in image cryptography for resource inadequate systems. Latest schemes, like Paillier cryptography, goal to alleviate this through developing homomorphic features that allow certain operations on cipher data devoid of decryption. These schemes assist safe processing but frequently need essential computational resources, building them minimum fit for less energy devoid of further optimization.

C. Chaotic Key Production

Chaotic maps [11, 13] have gotten notice for their strength to produce arbitrary sequences that improve the randomness of encryption keys. Chaotic systems like logistic system, are generally utilized because of their sensibility to primary conditions, which is perfect for producing maximum entropy keys. Various researchers proposed numerous logistic key production scheme that mix chaotic map with feedback procedure to vibrantly adjust key production related to network conditions [14].

These maps suggest a powerful replacement to conventional arbitrary number producer, particularly in circumstances where maximum entropy and fast key alteration are difficult. Yet, the practical development of logistic maps needs cautious deliberation of accuracy and computational effectiveness to evade performance bottlenecks.

D. Lightweight Cryptographic Strategies

In reply to the requirement for effective encryption in resource obliged circumstances, lightweight cryptographic strategies have been implemented [11]. Strategies like Sparx are devised to offer passable protection with less computational and storage needs. Several researchers computed numerous lightweight strategies for image cryptography in IoT systems, emphasizing Sparx for its equivalence between protection and competence.

These strategies frequently use diminished block lengths and abridged operations to reduce operation time and power expenses, building them fit for vibrant networks with minimum computational strength. Yet, the exchange between protection and computational competence ruins a crucial deliberation, as overly abridged schemes can be vulnerable to particular kinds of cryptanalysis attacks [7].

E. Hybrid Strategies

Hybrid encryption strategies merge the power of symmetric and asymmetric encryption strategies, frequently leveraging the rapidity of symmetric cryptography for information and the safety of asymmetric cryptography for key interchange. Existing researches have illustrated mixing chaotic key production through lightweight encryption schemes to improve both safety and competence [10].

Looking onward, potential research is anticipated to emphasis on advance optimizing these hybrid strategies, investigating machine learning methods for adaptive cryptographic schemes, and emerging protocols that improve protection devoid of conceding the effectiveness of dynamic networked tools [14].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1510

In ref. [1], this work illustrates an exclusive image encryption strategy for merging logistic map and fuzzy numbers. The logistic system offers great sensibility to primary conditions, developing a random cryptographic procedure. The utilization of fuzzy numbers appends an extra level of complexity, building it tough for illegal person to decrypt the image devoid of exact key. The strategy illustrates strength against several cryptanalysis attacks and is computationally competent, creating it appropriate for private communications over vibrant networks.

In ref. [2], this work offers an image encryption scheme that influences DNA rules merged beside a 2D logistic system. The 2D chaotic system produces logistic series utilized for image transformation and dispersion, while DNA rules alter image information into an organic series architecture, improving cryptographic complexity. This twin scheme enhances the protection and endurance to cryptanalysis examination, mostly in circumstances where trivial and effective cryptographic strategies are needed.

In ref. [3], this work presents an image cryptosystem that uses a 3D logistic Hopfield Neural Network in aggregation alongside arbitrary row-column transformation. The 3D logistic scheme produces complex key sequences that are retained to transpose and disperse image pixels excellently. This strategy advances from the essential volatility of logistic system, joined besides the neural network vibrant status updating, delivering tough encryption suitable for protected image delivery in vibrant network.

In ref. [4], this framework introduces a 3D chaotic system to produce logistic series for image encryption. The 3D system improves the cryptographic complexity through generating a multi-dimensional logistic nature that advances dissemination and confusion characteristics. The paper illustrates that this strategy suggests great resiliency to differential attacks and has minimum computational overhead, building it practical for real time fields in vibrant network circumstances.

In ref. [5], this paper presents a quick image cryptosystem that merges reordering and dispersal procedures utilizing a time delayed amalgamative hyper chaos system. The synchronized processing of reordering and dispersal improves encryption rate while managing tough privacy characteristics. The hyper chaos system [16] presents multi-dimensional logistic nature, expressively enhancing the randomness and privacy of cryptographic system against cryptanalysis attacks

In ref. [6], this strategy uses several logistic maps to produce complex keys for image cryptosystem. Through incorporating several logistic maps, the scheme enhances the arbitrariness and protection of cipher images. This research offers the efficient numerous logistic systems to oppose the statistical attacks, building it comfortable for protected message delivery in environments where vibrant updating are frequent.

In ref. [7], this work presents a Piecewise-Logistic-Sine (PLS) system based image cryptosystem, which merges the characteristics of chaotic and sine maps to produce tough logistic series. The PLS map improves the randomness of cryptographic process, achieving great protection and effective evaluation. This scheme is specially fitted for fields in vibrant networks where fast and robust encryption is necessary.

In ref. [8], this schemes merges transformation-dispersal beside logistic S-boxes and DNA rules for cipher images. The logistic S-boxes presents dynamic modification in the substitution procedure, while DNA rules integrate an additional level of complexity. This scheme generates a great stage of protection and reliability in contrary to statistical attacks, creating it a sustainable solution for image cryptosystem in vibrant and resource containing circumstances.

In ref. [9], this research work illustrates an image cryptosystem that merges DNA rules with spatiotemporal chaos. The DNA rules generates a latest path to permute the image information, while spatiotemporal chaos mix a vibrant and random component to cryptographic process. This amalgamation improves the protection and competence of encryption, building it fit for real time areas in vibrant network settings.

In ref. [10], this work demonstrates an image cryptography that uses 2DNA rules and a 2D chaotic system. The 2DNA rules permit for effective and protected image information delivery, while 2D chaotic system produces logistic series for cryptography. The amalgamative scheme certifies a great level of protection and evaluation complexity, fit for vibrant networks with rigorous resource contents.

Here, a comprehensive examination of several research works is represented, related to image cryptography with proposed techniques, performance parameters, advantages and limitations (Table 1).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1510

Table 1 Comprehensive Analysis of Research Papers

References	Proposed Techniques	Performance Parameters	Advantages	Limitations
[1]	The combination of logistic system and fuzzy numbers	Encryption efficiency, computational competence, differential attacks analysis.	Maximum volatility and privacy. Fit for vibrant network circumstances.	Highly complex to develop fuzzy system with logistic map.
[2]	2D chaotic system with DNA coding	Entropy, Key Sensibility, computational competence.	Maximum privacy because of DNA rules. Useful for real-time applications.	Intricacy in DNA series operations. Probable efficiency issues for huge datasets.
[3]	Row-Column Permutation based 3D logistic Hopfield Neural Network	Cryptanalysis attacks resiliency, computational competence.	Great attack resiliency. Valuable confusion of image pixels.	Maximum evaluation cost because of neural network processes.
[4]	Chaotic image encryption based on a 3D Logistic map.	Security examination, encryption rate, computational overhead.	Minimum computational overhead.	Probable deprivation in efficiency using multidimensional images.
[5]	Hyper chaos system	Encryption rate, attacks resiliency analysis.	Speedy and secure encryption. Statistical attack resilient.	Maximum resources needed. Combinatorial procedure developing complexity.
[6]	Several logistic systems.	Key production complexity, cryptography competence.	Improved arbitrariness and protection using several chaotic maps. Attack resiliency.	High computational complexity.
[7]	Piecewise-Logistic-Sine (PLS) System.	Security, encryption rate, key sensibility examination.	Merge potency of chaos and sine equations. Competent and private cryptography process.	PLS features tuning is difficult. If the PLS system is not accurately formed then it creates probable vulnerabilities.
[8]	DNA and logistic map based S-box	Entropy, computational competence.	Maximum protection using vibrant S-box and DNA rules.	Higher complexity and computational cost.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1510

References	Proposed Techniques	Performance Parameters	Advantages	Limitations
[9]	DNA rules merge with spatiotemporal logistic system.	Attack resiliency, encryption rate, entropy.	Logistic map based Robust encryption using DNA rules. Fit for vibrant applications.	Higher complexity and computational issues in huge images.
[10]	DNA rules and 2D logistic system.	Cryptography efficiency, attack resiliency.	2DNA based maximum protection using chaotic system.	Probable efficiency degradation with huge datasets.

F. Summary

➢ *Logistic Systems*

Several papers utilize logistic systems because of their essential randomness and sensibility to primary situations, which increase the protection of cryptographic procedure [1].

➢ *DNA Rules*

Amalgamation of DNA rules inserts an extra stage of protection and complexity but can add computational issues [10].

➢ *Efficiency*

While maximum schemes object to equivalence protection and computational competence, the complexity of few schemes can enhance evaluation overhead, specifically in resource containing circumstances [7].

➢ *Dynamic/Vibrant Networks*

The developed schemes are tailored for vibrant networks, concentrating on proposed methods are tailored for dynamic networks, focusing on compliance and reliability against several attacks. Moreover, the practical development of these strategies in real time areas may demand further optimization to manage the evaluation requirements effectively [5].

III. CONCLUSION AND FUTURE WORK

This literature survey has offered a broad assessment of computationally effective and arbitrary key-based image encryption in the framework of vibrant networks. Existing research expresses noteworthy growth in deploying well-organized schemes for image cryptography to focus on decreasing calculation overhead with maximum security, and feasibility. The espousal of arbitrary key-based schemes is developing gradually frequent because of their essential protection benefits over fixed key schemes to increase the information confidentiality. Survey highlights the significance of cryptographic techniques that familiarize to the vibrant behavior of current networks. The successful key administration and sharing schemes are vital for managing protect communication within vibrant network topologies and circumstances. Confirming scalability, improving computational competence, and maintaining key sharing in extremely vibrant circumstances are fields that compel further investigation. Additionally, as network progress and latest attacks arise, continuous originality in cryptographic schemes will be crucial. Future research should emphasize on obtaining developing dynamic and robust cryptographic structures that can effortlessly merge with rising network strategies. Furthermore, there is a requirement for uniform benchmarks to compute the efficiency and privacy of these image encryption solutions steadily.

REFERENCES

[1]. D. E. Mfungo, X. Fu, Y. Xian and X. Wang, “A Novel Image Encryption Scheme using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information”, Applied Sciences, MDPI, Vol. 13(7113), pp. 1-25, 2023.
[2]. F. Elamrawy, M. Sharkas, and A. M. Nasser, “An image encryption based on DNA coding and 2DLogistic chaotic map”, International Journal of Signal Processing, Vol. 3, pp-27-32, 2018.
[3]. W. Yao, K. Gao, Z. Zhang, L. Cui and J. Zhang, “An Image Encryption Algorithm based on a 3D Chaotic Hopfield Neural Network and Random Row-Column Permutation”, Frontiers in Physics, Vol. 11, pp. 1-14, 2023.
[4]. G. Ye, K. Jiao, C. Pan, and X. Huang, “An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map”, Hindawi Security and Communication Networks, pp-1-11, 2018. (https://doi.org/10.1155/2018/8402578)
[5]. Y. Shen, J. Huang, L. Chen, T. Wen, T. Li and G. Zhang, “Fast and Secure Image Encryption Algorithm with Simultaneous Shuffling and Diffusion based on a Time Delayed Combinatorial Hyperchaos Map”, Entropy, MDPI, Vol. 25(753), pp. 1-22, 2023.
[6]. M. Akraam, T. Rashid and S. Zafar, “A Chaos based Image Encryption Scheme is Proposed using Multiple Chaotic Maps”, Mathematical Problems in Engineering, Hindawi, Vol 2023, pp. 1-13, 2023.
[7]. S. Shao, J. Li, P. Shao, and G. Xu, “Chaotic Image Encryption using Piecewise-Logistic-Sine Map”, IEEE Access, Vol. 11, pp. 27477-27488, 2023.
[8]. Y. Tian, and Z. Lu, “Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation”, AIP Advances, pp-1-23, 2017.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL1510

[9]. C. Song and Y. Qiao, "A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos", MDPI, Entropy, vol. 17, pp-6954-6968, 2015. (doi:10.3390/e17106954)
[10]. A. H. Alrubaie, M. A. A. Khodher and A. T. Abdulameer, "Image Encryption based on 2DNA Encoding and Chaotic 2D Logistic Map", Journal of Engineering and Applied Science, Springer, Vol. 70 (60), pp. 1-21, 2023.
[11]. M. Usama, and N. Zakaria, "Chaos-Based Simultaneous Compression and Encryption for Hadoop", PLoS ONE, vol. 12(1), pp-1-29, 2017. (doi:10.1371/journal.pone.0168207)
[12]. O. Reyad, Z. Kotulski and W. M. A. Elhafiez, "Image Encryption using Chaos-Driven Elliptic Curve Pseudo-Random Number Generators", Appl. Math. Inf. Sci., Vol. 10, No. 4, pp-1283-1292, 2016. (http://dx.doi.org/10.18576/amis/100407)
[13]. P. K. Shukla, A. Khare, M. A. Rizvi, S. Stalin and S. Kumar, "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing", Entropy, MDPI, vol. 17, pp-1387 1410, 2015. (doi:10.3390/e17031387)
[14]. S. Y. Wang, J. F. Zhao, X. F. Li and L. T. Zhang, "Image Blocking Encryption Algorithm Based on Laser Chaos Synchronization", Journal of Electrical and Computer Engineering, Hindawi, pp-1-15, 2016.
[15]. T. S. Kumar and R. Venkatesan, "A new Image Encryption Method Based on Knight's Travel path and True random number", Journalof Information Science and Engineering, vol. 32, pp-133-152, 2016.
[16]. X. Tong, Y. Liu, M. Zhang, H. Xu and Z. Wang, "An Image Encryption Scheme Based on Hyperchaotic Ra, binovich and Exponential Chaos Maps", Entropy, MDPI, 17, pp-181-196, 2015. (doi:10.3390/e17010181)