International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02918
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Modern Cryptosystems for Color Image Encryption: Insights and Future Directions

Smitty V Isidhore[1], Dr. Sr. Mini T. V[2], Dr. Anil George K[3]

[1]Assistant Professor ,Department of Computer Science Carmel College (Autonomous), Mala, Kerala, India.
[2]Associate Professor ,Department of Computer Science, Sacred Heart College (Autonomous), Chalakudy, Kerala, India.
[3]Assistant Professor ,Department of Computer Science, St. Thomas College (Autonomous), Thrissur, Kerala, India

---

Abstract - In the current digital age, the widespread use of color images in areas like healthcare, surveillance, and multimedia communications has significantly increased concerns about image security. By incorporating a systematic approach following PRISMA guidelines, this paper presents a critical review of recent developments in cryptosystems used for color image encryption. Through a standardized examination of the state-of-the-art techniques, this review assesses techniques that ensure the authenticity, confidentiality, and integrity of color images. We focus on offering insights into current developments along with outlining potential directions for future research in the field of color image encryption. The vital aim of this study is to provide a comprehensive analysis of modern encryption algorithms, including chaotic maps, image scrambling, and hybrid techniques, and to evaluate their performance. The paper highlights the evolution of cryptographic methodologies for enhancing security, acceptance, and effectiveness in real-world applications.

***Keywords*:** Color Image Encryptions, PRISMA, Choas-based Encryption, Image Scrambling, Hybrid Cryptography, Digital Security.

1.INTRODUCTION

Color images play an important role in various areas, including social networking, healthcare, security, and entertainment [1–3]. The safety and security of image contents in the digital environment became an increased area of concern with the increased dependency on these. The increased capability of malicious attackers has raised the need for strong encryption frameworks to safeguard color images [4, 5]. Truthful digital communication by preventing malicious access to this visual information can be attained only by ensuring the confidentiality, integrity, and authenticity of images.

In some cases, like automated surveillance systems and healthcare diagnostics, where the data is directly linked to the decisions made, ensuring the safety of color images is of high importance. Any mistakes in ensuring the security of these data pose a high risk of financial losses, privacy violations, and system compromises. This paves the way for advanced cryptosystems for ensuring secure image encryption, thereby providing image safety.

The best solution to ensure the safety and integrity of the image data is cryptography [6-7]. But the use of conventional text encryption techniques on higher-dimensional and repetitive image data can be less reliable. So, the researchers in this field have come up with innovative cryptosystems, specifically designed for images, that ensure the safety of data being accessed by outside malicious attackers [8]. Image encryptions should highly focus on making the image into some structures that are visually not possible to understand without the proper decryption [8].

Cryptographic techniques can be broadly divided into symmetric and asymmetric methods. Symmetric cryptography uses a single key for encryption and decryption, so it is much faster and more efficient. However, the secure sharing of this symmetric key between the sender and the receiver can be risky. To tackle this issue, asymmetric cryptography utilizes a pair of keys, namely, a public and private key, to ensure secure key exchange without exposing the private key. To enjoy the advantages of both the cryptographic methods along with mitigating drawbacks, the researchers have recently come up with hybrid cryptosystems that combine aspects of both symmetric and asymmetric methods [9, 10].

Recently, more advanced approaches like chaos-based encryption and image scrambling were introduced to enhance color image security. The unpredictable nature of the chaos systems to generate pseudorandom sequences makes chaos-based encryption extremely difficult break by the attackers. Similarly, scrambling techniques make the image unintelligible by rearranging pixel positions by maintaining the structural layout and real information secured. Both the techniques offer different levels of computational complexity, making it suitable for several applications [11].

Additionally, both opportunities and challenges are presented by the growth of artificial intelligence and quantum computing for color image cryptosystems. The adaptability and robustness of encryption algorithms were increased by artificial intelligence, but the emergence of quantum computing threatens existing cryptographic methods. It raises concerns about developing better cryptosystems that are capable of withstanding quantum-based attacks. Considering these technological developments, this paper critically reviews the state-of-the-art cryptosystems for color image encryption, with a particular focus on recent advancements. We aim to address current challenges and explore future research directions to improve security and efficiency in this area.

2. BACKGROUND

2.1.Overview of Cryptography

Cryptography is used to encrypt and decrypt data to ensure privacy, integrity, authenticity, and non-repudiation. Text-based cryptographic algorithms where plain text is encrypted to cipher text through an algorithm and keys were mostly used by traditional cryptographic methods. However, the increased use of higher-dimensional and redundant data, such as images, has raised concern about developing dedicated methods for these data [13].

2.2. Evolution of Image Encryption Techniques

The increased use of digital images has increased the need to develop more complex algorithms for the safety of image data. In the starting phase, researchers integrated conventional algorithms like the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) to mitigate the issue. But the difference in the nature of images from plain text became inadequate to maintain the security of these data [14–16].

In the late 1990s and early 2000s, researchers started to come up with specialized cryptosystems to solve the conventional algorithm adaptability issues. In 2001, Fridrich et al. [17] established a breakthrough image encryption technique that became the base for more research in the future. Over time, several different dedicated approaches were proposed in the literature. One of the noteworthy improvements in the research was the inclusion of chaotic systems in the encryption, increasing the efficacy of the image encryption systems [18, 19].

Additionally, there has been a great increase in research using hybrid methods that combine more than a single model to overcome the image security problem. By combining methods, hybrid systems could solve the most challenges and also leverage the strengths of singular systems. Nowadays, most of the hybrid works are done on chaos-based methodologies for enhanced security and performance. The concern of researchers for hybrid systems also shows the quest to adapt to the growing complexity of digital images while opposing the attacks by the malicious intruders [20, 21].

2.3. Classification of Image Encryption Methods

Image encryption techniques can be generally classified into three types: symmetric, asymmetric, and hybrid encryption**.**

2.3.1. Symmetric Cryptography

If the same key is used for both encryption and decryption, we call it symmetric cryptography, as illustrated in Figure 1. Being simple, fast, and efficient, symmetric cryptography is highly reliable for real-time applications. However, the secure transmission of the encryption key remains a significant challenge. One of the highly exploited algorithms for symmetric image cryptography is the Advanced Encryption Standard (AES) [22]. There have been various versions and improvements suggested by the researchers on AES in the literature [23, 24].

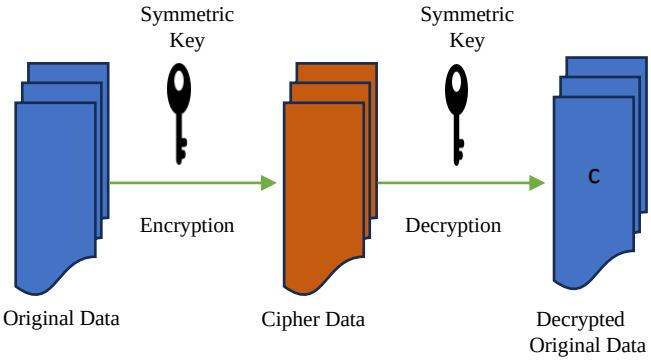

Figure 1. Symmetric Cryptography.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02918
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

2.3.2. Asymmetric Cryptography

If separate keys are used for encryption and decryptions, then the method is known as asymmetric encryption, as shown in Figure 2. Here the exchange of keys between the sender and receiver is much simplified, but the complete model requires more computational resources and tends to be much slower compared to symmetric methods. An asymmetric algorithm that is highly used for image encryption is Rivest-Shamir-Adleman (RSA). Often asymmetric algorithms are combined with symmetric or chaos-based systems to form a hybrid technique to achieve the best results in image encryption [25, 26].

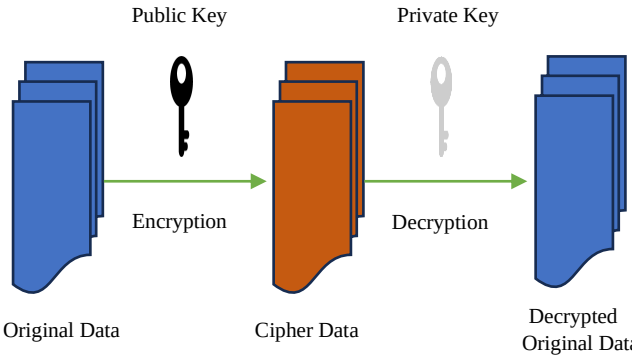

Figure 2. Asymmetric Cryptography

2.3.3. Hybrid Cryptography

When more than one approach is utilized for encryption, it is a hybrid cryptosystem. Hybrid cryptography often tries to make use of the strength of both symmetric and asymmetric encryption by integrating symmetric keys for fast encryption and asymmetric keys for secure key distribution. Recently, researchers have shifted to creating hybrid models by using more complex models such as chaos-based or image scrambling to further strengthen the safety and security of images [27, 28]. An example of a hybrid system, where data is encrypted using symmetric encryption and the symmetric key is encrypted with asymmetric encryption, is depicted in Figure 3.

Hybrid systems have become particularly relevant in securing color images due to their ability to balance efficiency and robust security measures. As the growing use of the internet and digital image keep on raising, there is a high need for advanced technology to resist modern attacks. Not only are the cryptography techniques getting evolved and better, but the threats are also evolving with the technological innovations. So, there is continuous innovation in cryptographic techniques, with hybrid and chaos-based systems at the forefront of recent developments [11, 29, 30].

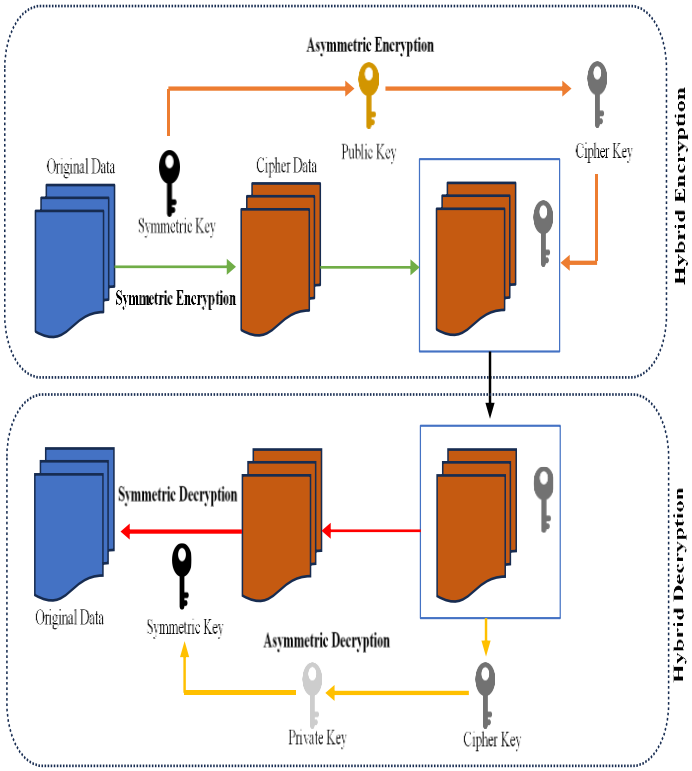

Figure 3. Example structure of hybrid cryptography

3. METHODOLOGY

The main purpose of this review is to analyze and summarize recent developments in color image encryption cryptosystems. To guarantee a thorough and objective selection of relevant study articles, we have followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) criteria.

3.1. Inclusion and Exclusion Criteria

3.1.1. Inclusion Criteria

- Papers published between 2020 and 2024
- Papers in English language only
- Peer-reviewed journal articles, conference papers, and open-access sources
- Select only papers in the field of Computer Science, Information Security, Cryptography
- Topic that only contains color image encryption

3.1.2. Exclusion Criteria

- Non-English papers
- Papers published before 2020
- Papers on cryptography beyond image encryption

3.2. Search Strategy

We have used Google Scholar for collecting research articles for our study. "Color image encryption" AND ("cryptography" OR "symmetric cryptography" OR "asymmetric cryptography" OR "chaos-based encryption" OR "image scrambling") were the search terms that were utilized. 7,590 results were found in this first search. To ensure only relevant articles are selected, we have used the following filters:

- Publication Year: The articles published between 2020 and 2024 were only selected to ensure articles were recent and not outdated. This filter has narrowed the results to 4,944.
- Document Type: We have eliminated review articles, editorials, and comments, which has eliminated 116 papers.
- Study Area: Priority was given to articles from the fields of computer science and cryptography.
- Open Access: Publicly accessible and open-access articles were only chosen, leaving 558 results.
- Sort on relevance: The articles were sorted using the relevance filter, and the first 250 were selected for further actions.

3.3. Screening Process

The titles and abstracts of the selected 250 articles was then read and 78 articles that we thought as irrelevant was excluded. The remaining 158 articles were considered from full-text reviewing. A thorough evaluation of these full-text articles was carried out to determine their relevance to our aimed subject. The final selected list consisted of 20 articles that were directly connected to the selected purpose and met all inclusion requirements. Figure 4 illustrates the PRISMA flow diagram in accordance with the article selection process, summarizing the identification, screening, and inclusion stages of the review.

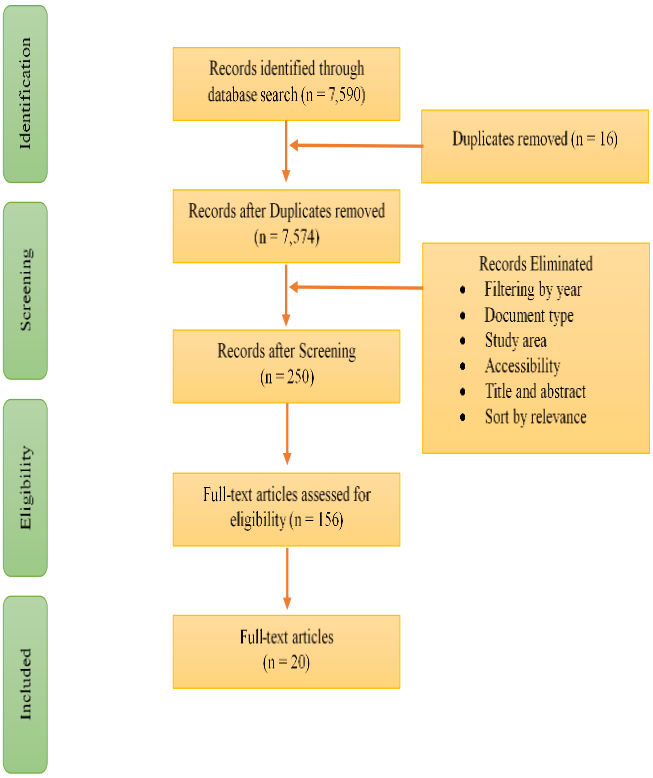

Figure 4. The PRISMA flow diagram.

4. RECENT ADVANCEMENTS IN COLOR IMAGE ENCRYPTION

The security aspects of color images in applications ranging from multimedia communications to healthcare and surveillance are crucial. Standard symmetric and asymmetric cryptographic algorithms, despite their widespread use, have drawbacks; therefore, current efforts focus on more sophisticated approaches like chaos-based and hybrid cryptosystems. In this section, we aim to provide a better analysis of the newest research in color image encryption, emphasizing the approaches, efficacy, and performance indicators.

4.1. Chaos Systems

Recent research on chaotic systems has been used to increase the security and randomness of approaches offered for image encryption. For example, in [33], a new strategy for color image encryption with 8x8 S-boxes, generated from a non-associative ring of order 512, was proposed. This design introduced the use of a 3D Arnold map for diffusion. Strong cryptographic features, including high nonlinearity and resilience to linear and differential attacks, were demonstrated.

In a similar manner, [36] examines a symmetric block cipher that employs a 4D-hyperchaotic map to produce three separate S-boxes of color channels. DNA encoding

was even used to boost security. Both feature unpredictability and chaotic aspects, making chaos-based cryptography vulnerable to a variety of assaults that can increase encryption security. However, while achieving a high entropy and minimal pixel correlation [33], the strategy of encoding with DNA was quite novel for boosting security levels, according to [36]. Furthermore, [48] discussed the use of a chaotic logistic map in conjunction with wavelet transforms to improve picture encryption security by increasing key sensitivity and entropy significantly.

Reference [46] proposes a new color image encryption technique based on DNA computing and double-chaos systems at the bit level. Arnold's approach initially scrambles three color components, followed by a Lorenz chaotic mapping and a fourth-order Rossler hyperchaotic mapping, both of which are utilized to generate chaotic diffusion sequences. This approach boosts the entropy of chaotic sequences to allow for the diffusion of high levels of bit-level color image, has a low computational overhead, and additional improvements in DNA coding rules support the durability of encryption performance.

[42] describes a novel technique to color image encryption based on a revolutionary four-dimensional (4-D) hyper-chaotic system. The secret key is generated using the SHA-256 hash method, which increases its security against known-plaintext assaults. The Arnold map is used for chaotic permutation, and the chaotic pseudo-random sequence is used to produce sophisticated S-boxes. Finally, the diffusive procedure is performed to the scrambled image utilizing the chaotic sequence, and it demonstrates great key sensitivity as well as robust security.

Another intriguing suggestion for a diffusion-based picture encryption technique employing chaotic maps is given in [43]. The method employs a chaotic map to build an S-box for pixel value modification, which is then diffused with a random sequence derived from the tent logistic chaotic map. It avoids the possibility of equal randomness distribution by mixing the color components of the pre-encrypted image, and thus yields promising security results.

Furthermore, [38] introduces a secure Elliptic Curve-based picture encryption and authentication paradigm for both grayscale and color images. The model generates a shared session key utilizing the secure Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol and an improved ElGamal encoding approach. Thus, the proposed model successfully scrambles and transforms plain picture pixels using 3D and 4D Arnold Cat maps, resulting in high-quality cipher images with low correlation for both types of images. It has proven to be strong against a variety of assaults, including statistical, differential, chosen-plaintext, known-plaintext, and occlusion.

[31] proposed a hybrid chaotic map approach based on matrix scattering for determining pixel location. The resilience to differential attacks was outstanding; nonetheless, the authors noted that this strategy may be excessive and unsuitable for live stream applications. Additional study by [49] demonstrated that various combinations, such as those employed in the Logistic and Sine maps, improve security while maintaining performance efficiency.

Another innovative idea was proposed by [37], who described a new encryption technique based on the picture dispersion principle and the Lorenz chaotic map. The approach used was to split the color of the pixels (Red, Green, Blue) by intermixing all of the channels vertically and horizontally, then splitting each into four regions and performing an XOR operation. Encryption is done in parallel with the RGB channels, and it is successful because the technique only takes a few milliseconds to complete both encryption and decryption. The NPCR, UACI, and entropy measures all returned positive findings. Security analyses revealed that it was resistant to differential attacks.

4.2. Hybrid Systems

Some recent studies used multi-stage or hybrid approaches to improve picture encryption performance. For example, [34] presented a method that used diffusion based on a chaotic logistic map as the first step, then substitution with the Hill cipher and color codes, and finally permutation using a piecewise chaotic linear map. When they compared their results to other recent approaches, they found high security metrics.

Recently, block-based encryption was employed in conjunction with logistic maps, 2D Arnold cat maps, and the Chen system. This method is distinguished by extremely low correlation coefficients and high resilience to differential attacks, emphasizing the need of multi-method methods in security enhancement.

Different perspectives on performance emerged. Multistage algorithms appear very promising, yet other publications suggest that complexity may be detrimental in practice. For example, in [36], the construction of super S-boxes for a four-dimensional chaotic system was reported, resulting in higher processing costs but more

resistance to known-plaintext attacks. In this regard, current research indicates that hybrid cryptosystems based on classical algorithms such as DES or AES can be combined with chaotic maps to achieve a significant balance between security and processing performance.

4.3. Comparative Studies

In [41], a comparison study assessed block cipher (AES), chaotic map (Arnold Cat Map), and hybrid chaotic map techniques. Such research discovered that, while AES provides strong security, it is less computationally efficient than its chaotic alternatives. While Arnold Cat Map provided very low resistance to differential attacks, hybrid chaotic map displayed exceptional immunity compared to the aforementioned approaches, with good NPCR and UACI values, but failed to retain picture quality under ideal conditions.

4.4. Innovative Encryption Techniques

There have been various recent ideas for novel approaches, with particularly interesting uses in image encryption. For example, in [39], two-stage encryption was given utilizing hyper-chaotic sequences; nonetheless, they are rather subject to statistical assaults. Furthermore, [40] developed an approach that uses the Lorenz system, S-box transformations, and Rule 30 cellular automata to achieve low correlation between nearby pixels while maintaining high entropy.

Another study [44] devised a novel image encryption technique that consists of five phases: the original color image is divided into eight segments, and the RGB matrices are scrambled by transforming them into binary code. This approach generated the secret key from the singer map and used the XOR logical operator for encryption, which was then reversed to decrypt. This approach has been exceedingly efficient in applying all tests, including entropy, correlation, UACI, and NPCR, and has offered adequate resistance to both attacks.

4.5. Applications in Internet of Things (IoT)

Another area of recent research is the implementation of picture encryption in IoT devices. In [45], a newly proposed lightweight symmetric cryptographic system established the concept of creating a unique session key for each image encryption procedure. When applied to IoT-based devices in the specific context, it proved more safe than standard algorithms. It also outperformed many existing algorithms using NPCR, UACI, and entropy.

Furthermore, in [47], a noisy environment was used, but an encryption scheme combining RSA and a Gaussian pyramid was used to improve image performance. The tremendous gain in visual quality and security demonstrated that encryption solutions must be developed to meet the specific constraints that IoT applications impose.

Advances in image cryptography provide new techniques and ideas, including chaotic systems, multi-stage procedures, and innovative approaches, all of which play a significant part in achieving safe solutions. It does not imply that more complex methods are used; rather, it refers to combining traditional techniques with more contemporary models, which is especially relevant in the context of IoT, to give even more safe and efficient methods for picture encryption. Table 1 provides a summary of the papers reviewed.

Table 1. Recent state-of-the-art summary.

Reference	Methodology	Feature
[31]	Matrix scrambling and hybrid chaotic map for pixel positions and key generation	Strong resistance to differential attacks, high entropy.
[32]	Hybrid crypto system integrating chaotic maps with traditional block ciphers.	High key sensitivity, resistance to differential attacks, uniform pixel distribution.
[33]	Color image encryption using 8×8 S-boxes generated from a non-associative ring	High nonlinearity, strict avalanche criteria, strong resistance to linear/differential attacks, high entropy.
[34]	Chaotic maps and color codes for encryption	High security against statistical and differential attacks, robust key space.
[35]	Block-based image encryption combining logistic maps, 2D Arnold cat maps, and the Chen system	Low correlation coefficients, high entropy, strong defense against differential attacks.
[36]	Symmetric block cipher using a 4D-hyperchaotic system	Effective key space, key sensitivity, strong reliability.
[37]	Image encryption based on image dispersion principle and Lorenz chaotic maps	Excellent efficiency, strong resistance to statistical and differential attacks
[38]	Elliptic Curve Cryptography (ECC) for image encryption and authentication	Strong defense against statistical attacks, low NPCR and UACI values.
[39]	Chaotic processes involving diffusion and confusion with hyper-chaotic sequences	High resistance against statistical attacks, efficient linear complexity.

[40]	Combining Lorenz system, S-box transformations, and Rule 30 Cellular Automata for encryption	Strong encryption performance, minimal pixel correlation.
[41]	4D chaotic system enhancing AES security	Effective for real-time image transmission systems, uniform distributions, minimal correlations.
[42]	4-D hyper-chaotic system with the SHA-256 hash algorithm	High key sensitivity and robust resistance to known-plaintext attacks.
[43]	Diffusion-based encryption algorithm that effectively combines chaotic maps with an S-box	Resistance against various attacks
[44]	Color image encryption using chaotic singer maps in a five-stage process	Strong security metrics, low pixel correlation.
[45]	Lightweight symmetric cryptographic algorithm for IoT-enabled devices	High NPCR and UACI values, low pixel correlation, uniform histogram distribution.
[46]	Integrating DNA computing with a double-chaos system for encryption	Strong resistance to various attacks, efficient bit-level diffusion.
[47]	Efficient color image encryption for IoT applications using RSA and Gaussian pyramid approach	Surpasses existing methods in visual quality and security under noisy conditions.
[48]	Lightweight image encryption using Corner Traversal Algorithm	Strong resistance to differential attacks, suitable for resource-constrained devices, adaptability and integration capability with various encryption schemes
[49]	Fast color image scrambling and encryption using hyperchaotic maps	Resistance against a variety of attacks, efficient for real-time applications.
[50]	Hybrid cryptosystem incorporating enhanced entropy algorithm	Fast and flexible, resistance to linear and algebraic attacks, good in maintaining visual quality.

5. LIMITATIONS AND FUTURE DIRECTIONS

By the advances in cryptographic techniques and rising need for secure communication in a wide range of applications, color image encryption is a rapidly growing field. According to several recent studies analyzed, the following are limitations and future directions obtained:

5.1. Limitations

- High computational complexity: Many advanced encryption techniques, particularly those based on chaotic and hybrid systems, are Computationally costly. This makes them impracticable for a numerous real-time application.
- Implementation Challenges: Some of the promising frameworks might not be so great in practical implementations. Specialized hardware or software needs may not be economical for all users and applications.
- Scalability: Some methods designed for individual photos may fail when used to massive datasets or dispersed cloud storage systems.
- Vulnerability: Because cyber threats are dynamic in nature, and current encryption techniques may be vulnerable to new attacks, encryption methods must always be updated and revised to successfully maintain the security and robustness.
- Dependence on key management: Most encryption techniques rely heavily on effective key management to provide security. Any flaws in creating, distributing, or maintaining keys may risk the security.

5.2. Future Directions

- Chaos and Hybrid Systems Integration: The study clearly indicates that chaos-based and hybrid cryptographic systems are growing. While integration appears to be beneficial in terms of security feature additions, performance metrics such as speed and key sensitivity are still a matter of concern. It will be good to include hybrid systems for use in real-time situations, particularly in activities that require higher speeds, such as multimedia communications and surveillance.
- Utilization of DNA Computing: The use of DNA computing in cryptographic methods, as mentioned in several research, is an interesting direction that could potentially contribute in the development of further security and efficiency.
- Quantum Cryptography: More research should be done to see how these quantum-resistant algorithms and protocols will safeguard color images from potential attacks by machines with quantum computing capabilities. This may require exploring quantum key distribution approaches to increase the security features of image encryption techniques.
- Weaknesses of existing techniques: With the exception of a few methodologies, the majority of methods have good security metrics. But, one main weakness is computational complexity and real-time implementation. Future research is expected to simplify encryption systems while maintaining the power of resilience measures. To

accomplish this, resource-constrained lightweight algorithms can be employed.

- Adaptation to IoT: Future research should concentrate on creating encryption algorithms specifically for IoT applications, where the selected energy consumption and processing rates are crucial.
- Collaboration Across Disciplines: The complexity of color image encryption necessitates a multidisciplinary approach. Collaborations between apparently disparate groups of researchers can result in innovative solutions that push the bounds of established cryptographic methods.

The future of color picture encryption looks promising, with numerous options to pursue that appear to lead to improved security as well as performance. This is because academics must consider new technologies and approaches, as well as the challenges that exist, in order to create a more secure digital landscape for color image transmission and storage.

6. CONCLUSION

The increased popularity of digital visual contents has raised concern for the secure communication of these data. Traditional encryption techniques often fail to achieve the needed security and robustness when it comes to color images. In recent years, there have been many advances in the area of color image encryption, including the development of chaos-based and hybrid cryptosystems. These methods have proven to be better solutions by providing enhanced security, integrity, and resistance to major attacks. However, processing complexity as well as the difficulty of real-time implementation and adaptability to new technologies still remain a concern. The future should focus on efficient algorithms that strike a balance between security and performance. Most significantly, they should be competitive enough to survive new cryptographic methods. Interdisciplinary techniques, along with cryptography, quantum computing, DNA computing, and machine learning, will be the keys to future advances. There is still the need for improvements in this field, as the data and communications are increasing day by day, as are the attacking strategies.

REFERENCES

[1] M. H. Noaman, H. Khaled, and H. M. Faheem, “Image colorization: A survey of methodolgies and techniques,” in Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2021, Cham: Springer International Publishing, 2022, pp. 115–130.

[2] Z. Mahmood, “Digital image processing: Advanced technologies and applications,” Appl. Sci. (Basel), vol. 14, no. 14, p. 6051, 2024.

[3] R. Archana and P. S. E. Jeevaraj, “Deep learning models for digital image processing: a review,” Artif. Intell. Rev., vol. 57, no. 1, 2024.

[4] A. P and W.-Z. Song, “Encryption algorithms for color images: A brief review of recent trends,” Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 10, 2016.

[5] Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis. .

[6] M. Ali and Dep. of Computer Science Ajloun National University Jordan, “A survey of the most current image encryption and decryption techniques,” Int. J. Adv. Res. Comput. Sci., vol. 10, no. 1, pp. 9–14, 2019.

[7] I. Haverkamp and D. K. Sarmah, “Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis,” Int. J. Inf. Secur., vol. 23, no. 4, pp. 2607–2635, 2024.

[8] A. Malik, S. Gupta, and S. Dhall, “Analysis of traditional and modern image encryption algorithms under realistic ambience,” Multimed. Tools Appl., vol. 79, no. 37–38, pp. 27941–27993, 2020.

[9] A. A.-R. El-Douh, S. F. Lu, A. Elkony, and A. S. Amein, “A systematic literature review: The taxonomy of hybrid cryptography models,” in Lecture Notes in Networks and Systems, Cham: Springer International Publishing, 2022, pp. 714–721.

[10] C. Paar, J. Pelzl, and T. Güneysu, Understanding cryptography: From established symmetric and asymmetric ciphers to post-quantum algorithms. Berlin, Heidelberg: Springer Berlin Heidelberg, 2024.

[11] K. M. Hosny, S. T. Kamal, and M. M. Darwish, “A color image encryption technique using block scrambling and chaos,” Multimed. Tools Appl., vol. 81, no. 1, pp. 505–525, 2022.

[12] P. Radanliev, “Artificial intelligence and quantum cryptography,” J. Anal. Sci. Technol., vol. 15, no. 1, 2024.

[13] W. Stallings, Cryptography and network security: Principles and practice, global ed, 8th ed. London, England: Pearson Education, 2022.

[14] J. Katz and Y. Lindell, Introduction to modern cryptography: Principles and protocols. Philadelphia, PA: Chapman & Hall/CRC, 2012.

[15] M. Singh and A. K. Singh, “A comprehensive survey on encryption techniques for digital images,” Multimed. Tools Appl., 2022.

[16] M. Kaur and V. Kumar, “A comprehensive review on image encryption techniques,” Arch. Comput. Methods Eng., vol. 27, no. 1, pp. 15–43, 2020.

[17] J. Fridrich, M. Goljan, and R. Du, “Invertible watermarking based on robust LSB substitution,” Proceedings of the IEEE International Conference on Image Processing, Thessaloniki, Greece, pp. 1–4, 2001.

[18] B. Zhang and L. Liu, “Chaos-based image encryption: Review, application, and challenges,” Mathematics, vol. 11, no. 11, p. 2585, 2023.

[19] N. Chaudhary, T. B. Shahi, and A. Neupane, “Secure image encryption using chaotic, hybrid chaotic and block cipher approach,” J. Imaging, vol. 8, no. 6, p. 167, 2022.

[20] Q. Zhang, “An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption,” in 2021 2nd International Conference on Computing and Data Science (CDS), 2021.

[21] U. S. M. Shah, “Hybrid image encryption techniques: A survey,” Journal of King Saud University - Computer and Information Sciences, vol. 33, pp. 345–356, 2021.

[22] Y. Alghamdi and A. Munir, "Image encryption algorithms: A survey of design and evaluation metrics," J. Cybersecur. Priv., vol. 4, no. 1, pp. 126–152, 2024.
[23] R. Wash and E. Rader, "Prioritizing security over usability: Strategies for how people choose passwords," J. Cybersecur., vol. 7, no. 1, 2021.
[24] M. Ramachandran, R. Patan, M. R. Babu, A. Kumar, and C. Thaventhiran, "Big data system based IoT enabling technologies: Ubiquitous wireless communication, real-time analytics, machine learning, deep learning, commodity sensors," in The Internet of Things and Big Data Analytics, Auerbach Publications, 2020, pp. 69–91.
[25] A. Desai, V. Parekh, U. Unadkat, and N. Shekokar, "Performance analysis of various asymmetric public-key cryptosystem," in Lecture Notes in Networks and Systems, Singapore: Springer Nature Singapore, 2023, pp. 437–449.
[26] R. Banoth and R. Regar, "Asymmetric key cryptography," in Classical and Modern Cryptography for Beginners, Cham: Springer Nature Switzerland, 2023, pp. 109–165.
[27] Aman and R. K. Aggarwal, "A survey: Analysis of existing hybrid cryptographic techniques," in Lecture Notes in Networks and Systems, Singapore: Springer Nature Singapore, 2024, pp. 259–269.
[28] M. Kumar, A. Saxena, and S. S. Vuppala, "A survey on chaos based image encryption techniques," in Multimedia Security Using Chaotic Maps: Principles and Methodologies, Cham: Springer International Publishing, 2020, pp. 1–26.
[29] Y. Cao and Y. Song, "Color image encryption based on an evolutionary codebook and chaotic systems," Entropy (Basel), vol. 26, no. 7, p. 597, 2024.
[30] Z. Bao, R. Xue, J. Hu, and Y. Liu, "Color image encryption based on lite dense-ResNet and bit-XOR diffusion," Multimed. Tools Appl., vol. 83, no. 5, pp. 12819–12848, 2023.
[31] A. K. H. Al-Ali and J. M. D. Alkhasraji, "Colour image encryption based on hybrid bit-level scrambling, ciphering, and public key cryptography," Bull. Electr. Eng. Inform., vol. 12, no. 3, pp. 1607–1619, 2023.
[32] S. W. Jirjees and A. T. Noor A Yousif, "Colour image privacy based on cascaded design of symmetric block cipher," J. Eng. Sci. Technol, vol. 17, pp. 2135–2156, 2022.
[33] N. Sanam, A. Ali, T. Shah, and G. Farooq, "Non-associative algebra redesigning block cipher with color image encryption," Comput. Mater. Contin., vol. 67, no. 1, pp. 1–21, 2021.
[34] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, "Analytic study of a novel color image encryption method based on the chaos system and color codes," Complexity, vol. 2021, no. 1, pp. 1–19, 2021.
[35] D. F. Chalob, A. A. Maryoosh, Z. M. Esa, and E. N. Abbud, "A new block cipher for image encryption based on multi chaotic systems," TELKOMNIKA, vol. 18, no. 6, p. 2983, 2020.
[36] H. Nazir, I. S. Bajwa, S. Abdullah, R. Kazmi, and M. Samiullah, "A color image encryption scheme combining hyperchaos and genetic codes," IEEE Access, vol. 10, pp. 14480–14495, 2022.
[37] M. Hassan and A. Kadhim, "New image encryption based on pixel mixing and generating chaos system," Al-Qadisiyah J. Pure Sci., vol. 25, no. 4, pp. 1–14, 2020.
[38] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," IEEE Access, vol. 9, pp. 76191–76204, 2021.
[39] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," Entropy (Basel), vol. 23, no. 3, p. 341, 2021.
[40] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, S-box and the Lorenz system," Symmetry (Basel), vol. 14, no. 3, p. 443, 2022.
[41] An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm. .
[42] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," Multimed. Tools Appl., vol. 81, no. 15, pp. 20585–20609, 2022.
[43] J. Chen, J. Tang, F. Zhang, H. Ni, and Y. Tang, "A NOVEL DIGITAL COLOR IMAGE ENCRYPTION ALGORITHM BASED ON A NEW 4-D HYPER-CHAOTIC SYSTEM AND AN IMPROVED S-BOX," Int. J. Innov. Comput. Inf. Control, vol. 18, no. 01, p. 73, 2022.
[44] A. B. Karim, P. S. Abdalqader, Z. T. Najim, A. M. Salhd, and O. Y. Abdulhammed, "Color image encryption with a novel technique and chaotic singer map," Science Journal of University of Zakho, vol. 9, no. 3, pp. 158–162, 2021.
[45] M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," Multimed. Tools Appl., vol. 80, no. 7, pp. 10391–10416, 2021.
[46] Q. Liu and L. Liu, "Color image encryption algorithm based on DNA coding and double chaos system," IEEE Access, vol. 8, pp. 83596–83610, 2020.
[47] S. Vishwakarma and N. K. Gupta, "An efficient color image security technique for IOT using fast RSA encryption technique," in 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2021.
[48] C. İnce, K. İnce, and D. Hanbay, "Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices," Multimed. Tools Appl., vol. 83, no. 29, pp. 72789–72817, 2024.
[49] Z. A. Abduljabbar et al., "Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map," IEEE Access, vol. 10, pp. 26257–26270, 2022.
[50] V. M. Silva-García, R. Flores-Carapia, and M. A. Cardona-López, "A hybrid cryptosystem incorporating a new algorithm for improved entropy," Entropy (Basel), vol. 26, no. 2, p. 154, 2024.