ISSN: 2581-3404 (Online) IF: 5.68 (SJIF)
IJIRTM, Volume-8, Issue-1, February-2024.

A Detailed Survey of Color Image Encryption Standards (IES)

Mahak Saxena[1], Kaptan Singh[2] and Amit Saxena[3]
[1] Truba Institute of Engineering & Information Technology, Bhopal, India, 462038
[2]Truba Institute of Engineering & Information Technology, Bhopal, India, 462038
[3]Truba Institute of Engineering & Information Technology, Bhopal, India, 462038
[1]mickey.saxena3@gmail.com, [2]kaptan2007@gmail.com, [3]amitsaxena@trubainstitute.ac.in

Abstract. *Color image encryption is an essential domain within the realm of information security, ensuring the confidentiality and integrity of visual data transmitted over networks or stored in digital form. This paper presents a comprehensive survey of existing color image encryption standards (IES), examining their methodologies, strengths, weaknesses, and applicability across diverse scenarios. By systematically reviewing prominent encryption techniques tailored specifically for color images, this survey aims to provide researchers and practitioners with a structured understanding of the state-of-the-art in color image encryption. Through a detailed analysis of various standards, including their encryption algorithms, key management strategies, and performance metrics, this paper offers insights into the evolving landscape of color image security. Additionally, it discusses emerging trends and potential avenues for future research, thereby facilitating advancements in the development of robust and efficient color image encryption solutions.*

Keywords:- Image encryption, Decryption, Latin square, Security, Algorithms.

Introduction

Securing images has emerged as a critical facet of safeguarding data [1]. To tackle this issue, researchers and professionals are focusing on devising and exploring efficient image encryption and security standards. Cryptography stands out as the dominant approach employed to protect digital photographs. Cryptography utilizes mathematical algorithms and methods to convert data into a secure and indecipherable format, thereby rendering it difficult for unauthorized individuals to access or decipher the original content [2]. This recognition comes amidst the increasing reliance on digital data, especially during pandemics, when digital interactions surge. With heightened digital engagement, the imperative to secure various forms of data, including images, becomes more pronounced. The emphasis on image security is crucial, acknowledging that images frequently harbor sensitive or valuable information [3]. Safeguarding this visual data is indispensable to thwart unauthorized access, tampering, or theft. Consequently, there is a growing demand for the advancement and exploration of effective image encryption techniques [4]. Image encryption entails converting image content into a secure and incomprehensible form to shield it from unauthorized access. Cryptography is singled out as the primary approach for fortifying digital photographs, employing cryptographic algorithms and techniques to encode image content, thereby fortifying them against unauthorized access. Within the cryptography domain, specific tools known as cryptographic ciphers are utilized to encode images [5]. These ciphers function using cryptographic keys, which are pivotal for both

encryption and decryption processes. The emphasis is placed on the use of secure keys, which are indispensable in the cryptographic process, as they facilitate the encoding and decoding of images. The security of the entire system hinges on the strength and confidentiality of these keys. To sum up, the statement underscores the significance of addressing image security concerns, advocates for the advancement of effective image encryption techniques, and identifies cryptography, particularly cryptographic ciphers with secure keys, as the primary means to accomplish this objective.

II. Encryption & Decryption

Since antiquity, the practice of encrypting crucial messages has been employed to prevent unauthorized access, particularly in contexts such as military communications during warfare [6]. In our contemporary era, characterized by widespread computing, internet usage, and technological services facilitating data storage, communication, financial transactions, the risk of data theft and forgery has escalated, underscoring the heightened necessity for encryption methods to safeguard messages and sensitive data. Encryption is delineated as a specific technique for securely transmitting data between two parties, ensuring non-interference from unauthorized third parties [7]. It relies on a designated algorithm, message, and key for both encryption and decryption processes. Encryption functions by transforming the message into an unintelligible format, with decryption restoring the message to its original state when the appropriate key is utilized. The plaintext denotes the original message, while the encrypted message is termed ciphertext. Encryption serves to fortify information systems, hardware, and software, aligning with the primary objectives of computer security encapsulated in the CIA triad: confidentiality, integrity, and availability [9]. Confidentiality underscores the importance of information privacy, ensuring that data remains under the control of authorized individuals and limiting access solely to authorized parties. Integrity safeguards data against unauthorized alterations, preserving data integrity, and ensuring the proper functioning of systems, termed system integrity. Availability pertains to guaranteeing uninterrupted access to required services for users, without any disruption or denial of service [10].

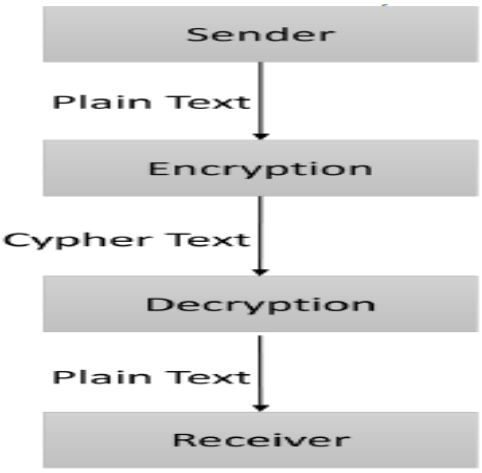


Fig. 1: Encryption & Decryption Method.

Algorithms for encryption and decryption can be categorized into two main types: symmetric algorithms and asymmetric algorithms. Symmetric algorithms utilize the same key for both encryption and decryption processes, ensuring that the sender and receiver possess identical keys [11]. Conversely, asymmetric algorithms utilize a different key for encryption (known only to the sender) and decryption (known only to the receiver), enhancing security through this key separation [11]. To bolster algorithmic security, considerations are made regarding potential brute force attacks, where adversaries attempt to guess passwords by exploiting knowledge of the encryption algorithm. Consequently, algorithms vie in terms of the strength and efficiency of the keys utilized for message encryption and decryption [11]. Traditionally, encryption techniques encompass substitution and transposition. Some algorithms exclusively employ substitution, while others solely rely on transposition. Additionally, certain algorithms integrate both techniques to heighten security and increase the complexity of decrypting data. Beyond encryption, the concept of steganography has emerged, offering an alternative approach to conceal messages. Steganography involves hiding the content of a message within another medium, such as embedding text within an image, without altering the appearance of the original medium. This method aims to obscure the presence of the message altogether, augmenting the layers of security for sensitive information.

III. Image Encryption Standards (IES)

Classic Image Encryption- an improved AES based "Classic Image Encryption" algorithm enhances AES-based encryption for image processing by integrating a key stream generator (such as A5/1 or W7) with AES, thereby enhancing encryption performance. This improvement ensures a more robust encryption process for images. Keys are independently generated at both the sender and recipient ends, based on AES Key extension transformation. Consequently, only the initial key is shared, rather than the entire set of keys [12].

Public Key Image Encryption- In scenarios where a secure channel for transferring private keys is unavailable or where the decryption key must remain secret, "Public Key Image Encryption" utilizes public key cryptography. Initially proposed by Diffie and Hellman, this method enables the creation of a shared secret key over a secure communication channel without prior key sharing. Traditional public key cryptosystems are primarily designed for encoding textual data. In this scheme, the plain image is divided into blocks using a specific grid transformation, and all pixels within each block are then transferred to the Discrete Cosine Transform (DCT) domain. Encryption and decryption procedures are defined based on the transformation grid of DCT coefficients [13].

Compression and Encryption- This techniques aim to reduce transmission bandwidth or storage space. These techniques can be implemented in both spatial and frequency domains, with frequency domain methods typically being more efficient. Lossy compression methods trade a certain loss of information for higher compression ratios, making them suitable for images, videos, and audio data. Lossless compression methods, on the other hand, ensure no loss of data quality, making them suitable for preserving data integrity in scenarios such as database records, executable files, and medical images. Lossy coding methods include predictive coding and transform coding, while lossless coding methods include run-length encoding, Huffman encoding, arithmetic encoding, entropy coding, and area coding. However, integrating ordinary cryptosystems with compressed multimedia presents challenges, as encrypting multimedia content before

compression can reduce compression efficiency, while encrypting data after compression can disrupt codec patterns [14, 15].

Selective Encryption- This techniques aim to avoid encrypting the entire image, thereby reducing computational overhead for real-time applications without compromising data security. Selective encryption divides image content into public and protected shares, with a focus on minimizing the encrypted portion. Typically, selective encryption is accompanied by compression, with low-frequency coefficients containing most image data and high-frequency coefficients conveying finer details [16]. These techniques collectively contribute to improving the security and efficiency of image encryption and compression processes.

IV. Classification of Various IES Methods

With the increasing use of digital data during pandemics, image security has become a prominent concern in the contemporary scenario. Consequently, effective image encryption and security standards must be designed and researched. Cryptography is the most common method employed to protect digital photographs. Cryptographic ciphers are utilized to encode images with secure keys. Latin Square (LS) based image encryption standards [17] offer an efficient means of reducing process memory requirements. Numerous Latin Square cipher-based image encryption standards [18] have been developed to enhance security standards. Typical block-based encryption schemes have limitations such as a restricted image size of (256x256) and reliance on pixel-level information, which can compromise recovery quality. It is crucial to enhance the performance of encryption standards when confronted with various threats, particularly noise. Several chaotic Image encryption algorithms (IEA) [18] have been introduced in the past.

Figure 2 provides a brief classification of various IEA methods based on the block ciphers and chaos used for image encryption. The most widely used image encryption methods, as classified, are LS, Advanced Encryption Standard (AES), and Data Encryption Standard (DES). The primary concern of this paper is to design accurate Latin Square (LS) image ciphers for encryption.

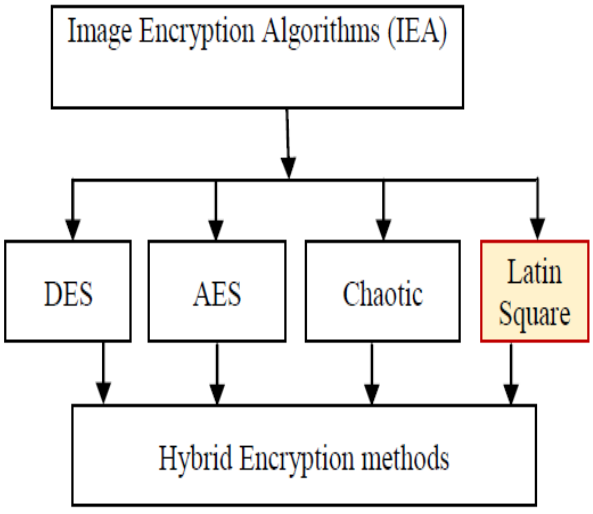


Fig. 2: Classification of color image encryption methods.

Many hybrid approaches that combine various encryption standards have also been developed in the past. Image security is achieved through a combination of picture decryption and encryption. Latin square (LS)-based encryption algorithms have been employed as efficient and secure picture security standards.

V. Summary of Color Image Security Algorithms

Yue Wu et al. [1] presented a symmetric-key-based Latin square image ciphering method for both color and grayscale images. They introduced a new LS encrypted image based on the concepts of Latin Round Bleaching (LEB), Latin Round S-box, and LS P-box. These fresh Latin-centered image encoding methods are combined to create an LS image cipher using a single turned LS novel loom-like substitution-permutation system. Ali et al. [2] utilized chaos maps to provide a diffusion-driven image encryption method. They used an unstable chaos map to construct an S-box and modify pixel values to create a nonlinear component. These modified values were further dispersed using a different sequence of events generated using an inflatable logistical chaos map. Ming Xu et al. [3] proposed an innovative encryption technique using self-orthogonal LS research. Self-orthogonal Roman squares can produce specific 1D/2D maps for image combinations and offer a pseudo-random pattern for shuffling images. Based on simulation findings, this method is suitable for real-world implementation as it is both secure and efficient. A. H. Abdullah et al. [4] examined an evolutionary encryption approach that was recently developed. They proposed a unique photograph encryption technique that relies on a combination of genetic algorithms (GA), stochastic maps, and a DNA (deoxyribonucleic acid) mask. Zhang X et al. [5] employed Italian rectangles produced using chaotic sequences in their algorithm for encryption. This approach increased the complexity of the resulting Latin cube matrices and strengthened the algorithm's reliability. Shen et al. [6] introduced a novel stackable architecture for encrypting images that offers superior security and efficiency. They utilized a Latin rectangular, and an n-transversal can yield two perpendicular rectangles in addition to classifying every place in the data matrix. X. L. Chai et al. [7] introduced an updated Hénon map and demonstrated that it is more complex and exhibits richer chaotic behaviors through dynamic analysis. They used the modified Hénon patterns to build an encryption system for color images. G. Q. Hu et al. [8] proposed a bit-level turbulent image cipher based on lookup tables to enhance efficiency and address the limitations of traditional methods. H. T. Panduranga et al. [9] introduced an unstructured map and Latin cube picture cipher-based permutation-substitution encryption of images system, using a chaotic map for the transformation process. Kanaad Deshpande et al. [10] presented a new method of encrypting photos using a Sudoku puzzle as the encryption key, compatible with various keyspaces, Sudoku sizes, and data types. A.V. Diaconu et al. [11] studied a method that uses a Sudoku puzzle as the encryption key, functioning with any keyspace, puzzle size, and data format, and employing a pseudo-random integer from the Sudoku puzzle as a threshold value. Arora et al. [12] focused on the series of the wfsr and its role in image encryption, emphasizing the need to select specific plain and cipher picture pairs to invert the arrangement of the Arnold conversion and the logistical mapping. Nora Almalki et al. [13] emphasized the secure storage of health information in the face of advancing medical technology and the use of cloud storage. Haixiao Li et al. [14] introduced a picture encryption method based on cross-plane zag transformation and an enhanced lifting-like architecture, addressing issues with the initial structure's simplicity. Zarei Zefreh et al. [15] presented LSIE, a fast and secure image encryption method based on Latin squares that utilizes chaotic structures and the SHA256 hash algorithm. Tanvi Nema et al. [16] acknowledged the importance of data

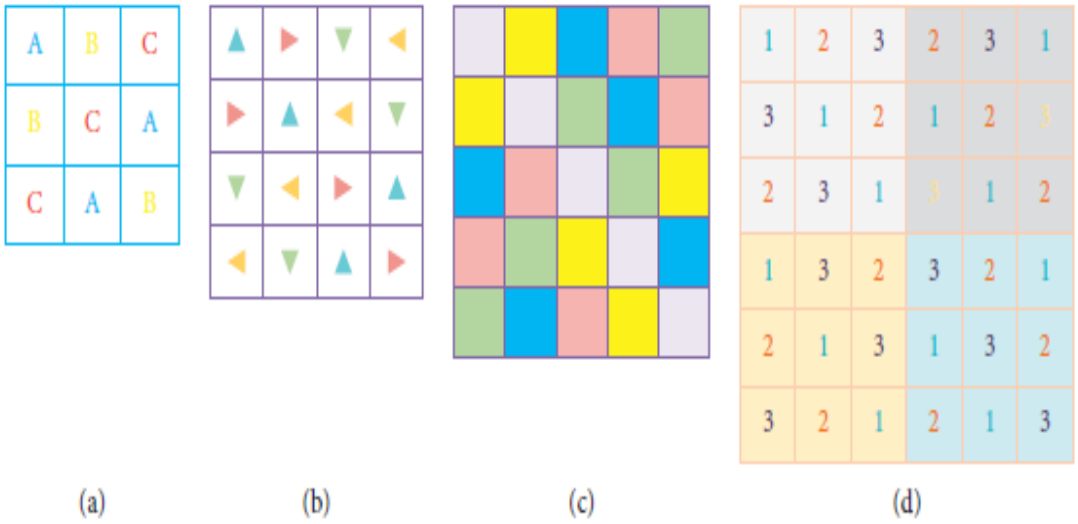
protection in the context of confidentiality and security issues in the field of computers and emphasized cryptography as a viable technology for safeguarding interactions and stored information.

Table 1: Summary of some color image security algorithms.

Authors and Reference	Encryption Method Description
Yue Wu et al. [1]	Symmetric-key-based Latin square image ciphering method using Latin Round Bleaching, Latin Round S-box, and LS P-box for color and grayscale images.
Ali et al. [2]	Diffusion-driven image encryption method utilizing chaos maps and unstable chaos map for constructing S-box.
Ming Xu et al. [3]	Encryption technique using self-orthogonal LS research, generating specific 1D/2D maps for image combinations.
A. H. Abdullah et al. [4]	Evolutionary encryption approach combining genetic algorithms (GA), stochastic maps, and a DNA mask.
Zhang X et al. [5]	Encryption algorithm employing Italian rectangles produced using chaotic sequences to enhance complexity.
Shen et al. [6]	Introduction of a novel stackable architecture for image encryption using Latin rectangular and n-transversal.
X. L. Chai et al. [7]	Encryption system for color images using an updated Hénon map, exhibiting richer chaotic behaviors.
G. Q. Hu et al. [8]	Bit-level turbulent image cipher based on lookup tables for efficiency enhancement.
H. T. Panduranga et al. [9]	Unstructured map and Latin cube picture cipher-based permutation-substitution encryption of images.
Kanaad Deshpande et al. [10]	Encryption method using a Sudoku puzzle as the key, compatible with various keyspaces and puzzle sizes.
A.V. Diaconu et al. [11]	Method using a Sudoku puzzle as the encryption key, working with any keyspace, puzzle size, and data format.
Arora et al. [12]	Focus on the wfsr series and its role in image encryption, highlighting the need for specific plain and cipher picture pairs.
Nora Almalki et al. [13]	Emphasis on secure storage of health information, considering advancing medical technology and cloud storage.
Haixiao Li et al. [14]	Picture encryption method based on cross-plane zag transformation and an enhanced lifting-like architecture.
Zarei Zefreh et al. [15]	LSIE, a fast and secure image encryption method based on Latin squares using chaotic structures and SHA256 hash algorithm.
Tanvi Nema et al. [16]	Acknowledgment of data protection importance in the context of confidentiality and security issues, emphasizing cryptography.

VI. Latin Square

The concept of Latin squares, named after the renowned mathematician and physicist Euler, stems from his utilization of the Latin alphabet to represent elements within the square. A Latin square matrix is defined as an N×N matrix comprising N distinct elements, with each element appearing precisely once in every row and column. This property distinguishes Latin square matrices and underscores their significance in various applications. One prominent application of Latin square matrices lies in image processing, particularly in enhancing the distribution and balance of pixels within an image matrix. By employing Latin squares, the row and column vectors of the image matrix undergo double control, leading to a more uniform distribution of pixels across the matrix. This process contributes to improving the overall balance and quality of the image representation. Figure 3 illustrates examples of Latin squares featuring different symbol sets, showcasing the versatility and applicability of this mathematical construct in various contexts, including image processing. Through the integration of Latin squares, image processing techniques can achieve enhanced pixel distribution and matrix balance, thereby improving the visual quality and integrity of images.



(a) 3 × 3. (b) 4 × 4. (c) 5 × 5. (d) 9 × 9.

Fig. 3: Latin square example.

The concept of a Latin square involves arranging symbols from an alphabet of size n in cells so that each symbol appears only once in each row and column. This term originates from the work of Leonhard Euler, who utilized Latin characters as symbols in his mathematical papers. Building upon the theory of Latin squares, we have developed the Latin Square Image Cipher (LSIC) based on the research presented by Yue Wu [10]. To generate LSIC, we employ a key comprised of 64 hexadecimal characters, corresponding to a total length of 256 bits. Each hexadecimal character represents 4 bits. Thus, the provided key is "F5A172A6E8B163D987C23A78B12F73A6519D76C53B12A64CC67B8981267ABFD". Figure 4 illustrates the Latin Square Image Cipher generated using the aforementioned 256-bit key, along with its

corresponding histogram. This cipher serves as a cryptographic technique for securing image data, leveraging the principles of Latin squares to enhance encryption efficacy and maintain data integrity. Through the utilization of LSIC, sensitive image data can be protected from unauthorized access and manipulation, ensuring confidentiality and security.

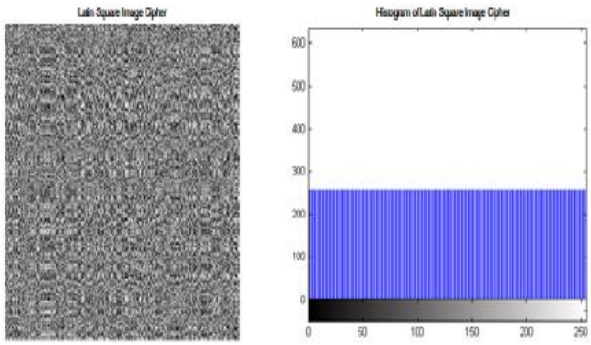


Fig. 4: Latin Square Image Cipher and Histogram.

VII. Security Analysis of Encrypted Image

The shortcomings of a cryptosystem can lead to the recovery of either the entire or a portion of a ciphered message (such as an image) or the discovery of the secret key without knowledge of the decryption key or algorithm. Various methods can be employed to investigate these vulnerabilities, depending on the access the attacker has to plaintext, ciphertext, or other components of the cryptosystem. Here are some of the most common types of attacks on encrypted images:

Key Space Analysis- This attack attempts to find the decryption key by systematically checking all possible keys. The number of attempts required to find the key, known as the key space, increases exponentially with the total key size. For instance, doubling the key size quadruples the number of required operations. Therefore, a cryptosystem with a 128-bit key size defines a key space of 2^{128}, which is computationally infeasible to brute force with current technology.

Statistical Analysis- By analyzing data statistically, relationships between the original and encrypted images can be inferred. According to Shannon's theory, encrypted images should be completely indistinguishable from the original. However, statistical analysis can often reveal information leakage from the encrypted image, compromising its security.

Correlation Analysis- In plain images, adjacent pixels exhibit strong correlations both vertically and horizontally. A strong encrypted image should have a correlation coefficient close to 0, indicating that there is no discernible relationship between adjacent pixels.

Differential Analysis- This method aims to determine the sensitivity of an encryption algorithm to minor changes. If a small change is made to the plaintext image, the resulting encrypted image should exhibit significant changes, making it difficult to discern any relationship between the original and encrypted images.

Key Sensitivity Analysis- In addition to having a large key space to resist brute force attacks, a secure algorithm should also be highly sensitive to changes in the secret key. Even slight alterations to the key should render the encrypted image completely indecipherable.
These types of attacks highlight the importance of designing robust encryption algorithms and employing secure cryptographic practices to protect sensitive information in images and other data.

VIII. Security Analysis of The Encryption Schemes

Security analysis involves identifying weaknesses in a cryptosystem and recovering either the entire or a part of a ciphered image or finding the secret key without knowledge of the decryption key or algorithm. Various techniques are available for conducting such analysis, depending on the access the analyst has to the plaintext, ciphertext, or other aspects of the cryptosystem. Some common types of attacks on encrypted images include:
Key Space Analysis- This attack involves attempting to find the decryption key by checking all possible keys. The key space of the cryptosystem grows exponentially with increasing key size, making brute force attacks computationally infeasible. A larger key size enhances the robustness of the cryptosystem against such attacks.
Key Sensitivity Analysis- A good image encryption scheme should be sensitive to changes in the secret key used. Even a small change in the key should result in a completely different encrypted or decrypted image, enhancing security.
Statistical Analysis- Statistical analysis examines the relationship between the original and ciphered images. Histograms and correlations of adjacent pixels in both plain and encrypted images are used to analyze the encryption scheme's statistical characteristics. If the histograms of the encrypted image resemble those of a random image, the encryption algorithm is considered to perform well.
Correlation Coefficient Analysis- This analysis studies the correlation between adjacent pixels in the plain and encrypted images. High correlation values in the plain image indicate a strong relationship between adjacent pixels, whereas in the encrypted image, correlations are typically minimal. Significant differences in correlation values indicate effective encryption.
Information Entropy Analysis- Entropy analysis tests the robustness of the encryption algorithm. Comparing the entropy of plain and encrypted images helps evaluate the algorithm's ability to resist entropy attacks. A high entropy value in the encrypted image indicates strong encryption.
Differential Analysis- This analysis aims to determine the sensitivity of the encryption algorithm to minor changes in the plain image. Measures such as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) assess the impact of small changes on the encrypted image. High NPCR and UACI values indicate resistance against differential attacks.
By employing these various analysis techniques, cryptographers can evaluate the strength and effectiveness of encryption algorithms and enhance the security of encrypted images.

IX. Conclusion and Future Scope

In conclusion, this detailed survey has shed light on the diverse landscape of color image encryption standards (IES), providing a comprehensive overview of existing methodologies, techniques, and performance metrics. Through a systematic examination of prominent encryption standards, including their

strengths, weaknesses, and applicability, this study has contributed to a better understanding of the state-of-the-art in color image security. The survey has revealed the complexities involved in securing color images, considering factors such as encryption algorithms, key management strategies, and performance benchmarks. While existing standards offer various levels of security and efficiency, there remains.

Overall, this survey serves as a valuable resource for researchers, practitioners, and policymakers involved in the development and deployment of color image encryption solutions. By fostering a deeper understanding of existing standards and emerging trends, this study aims to catalyze advancements in the field of color image security, ultimately contributing to the protection of sensitive visual data in various domains.

References

[1] Yue Wu, Yicong Zhou, Joseph P. Noonan, SosAgaian, and C. L. Philip Chen, "A Novel Latin Square Image Cipher", a draft submitted to IEEE transactions on information forensics and security. 2014.

[2] Ali, T.S., Ali, R.,"A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box", Multimedia Tools &Appl, 81, 20585–20609 (2022). https://doi.org/10.1007/s11042-022-12268-6

[3] Ming Xua,,ZihongTiana, "A Novel Image Encryption Algorithm Based on Self-orthogonal Latin Squares", Journal of Optik (2018).

[4] H. Abdullah, R. Enayatifar, M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption", AEU-International Journal of Electronics and Communications. 66(10) (2012)806-816

[5] Zhang X, Wu T, Wang Y, Jiang L, Niu Y.,"A Novel Chaotic Image Encryption Algorithm Based on Latin Square and Random Shift. Comput Intell Neurosci" 2021, Sep 6;2021:2091053. doi: 10.1155/2021/2091053. PMID: 34531907; PMCID: PMC8440112.

[6] Shen, H.; Shan, X.; Xu, M.; Tian, Z.,"A New Chaotic Image Encryption Algorithm Based on Transversals in a Latin Square", Entropy 2022, 24, 1574. https://doi.org/10.3390/e24111574

[7] X. L. Chai, Z. H. Gan, K. Yang, Y. R. Chen, X. X. Liu, "An image encryption algorithm based on the memristivehyperchaotic system, cellular automata and DNA sequence operations", Signal Processing: Image Communication. 52, 6-19. (2017)

[8] G. Q. Hu, D. Xiao, Y. S. Zhang, T. Xiang, "An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy", Nonlinear Dynamics. 87(2) , 359-1375., (2017)

[9] H. T. Panduranga, N. Kumar, S. K. Kiran, "Image encryption based on permutation-substitution using chaotic map and Latin square image cipher", The European Physical Journal-Special Topics. 223, (8) 1663-1677 , (2014)

[10] Kanaad Deshpande, Junaid Girkar & Ramchandra Mangrulkar, "Security enhancement & analysis of images using a novel Sudoku based encryption algorithm", Journal of Information and Telecommunication, 2023, 7:3, 270-303.

[11] Y. Zhang, Y. S. Liu, C. Wang, J. T. Zhou, Y. S. Zhang, G. R. Chen, "Improved known-plaintext attack to permutation-only multimedia ciphers", Journal of Information sciences. 430-431, pp. 228-239, (2018)

[12] A.V. Diaconu, "Circular inter-intra pixels bit-level permutation and chaos-based image encryption", in Journal of Information Sciences. 355-356, pp 314-327, (2016)

[13] Arora, A., Sharma, R.K.,"Cryptanalysis and enhancement of image encryption scheme based on word-oriented feedback shift register", Multimedia Tools&Appl, 81, 16679–16705 (2022).
[14] Nora Almalki and HatimAlsuwat, "A Systematic Literature Review on Security Challenges In Image Encryption Algorithms for Medical Images", IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.6, June 2022
[15] Haixiao Li, Yinan Hu, Ziming Shi , Bin Wang , And Pan Zheng, "An Image Encryption Algorithm Based on Improved Lifting-Like Structure and Cross-Plane Zigzag Transform", VOLUME 10, 2022 IEEE ACCESS.
[16] ZareiZefreh, E., Abdali, M.,"LSIE: a fast and secure Latin square-based image encryption scheme", Multimedia Tools &Appl (2023). https://doi.org/10.1007/s11042-023-14786-3
[17] TanviNema, Prof. Amitnandanwa, "A Symmetric-Key Latin Square Image Cipher with Probabilistic Encryption for Grayscale and Color Images", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 8 (3) , 2017, 380-388 .
[18] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad UsmanHashmi, QaisarShaheen, Rizwan Akhtar and Allah Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing",Hindawi Security and Communication Networks Volume 2020, Article ID 8863345, 16 pages.https://doi.org/10.1155/2020/886334.