ISSN: 2096-3246
Volume 58, Issue 02, 2026

A QUANTUM-RESISTANT FRAMEWORK FOR SECURE RGB IMAGE TRANSMISSION USING ADVANCED COMPUTATIONAL TECHNIQUES

Rajesh Kumar Tiwari[1], Prabhjot Kaur[2] , Ritu Mishra[3] , Kanchan Nahar[4], Bhushan[5],Ashok Singh Gaur[6]

[1] Dr. Ambedkar Institute of Technology for Divyangjan, Kanpur, Uttar Pradesh, India
srohittiwari091@gmail.com
[2]School of Advanced Computing (SAC), CGC University, Mohali – 140307, Punjab, India
pjmahi8@gmail.com
[3]MMICT&BM, Maharishi Markandeshwar (deemed to be university)
ritu.mishra8168@gmail.com
[4]MMICTBM, Maharishi Markandeshwar (deemed to be university)
Kanchannahar16@gmail.com
[5]Department of Computer Application, Sgt university Gurugram
bhushan_soet@sgtuniversity.org
[6] Noida Institute of Engineering and Technology, Greater Noida
ashok07mc03@gmail.com

Abstract

Digital RGB images are widely used in applications such as medical imaging, surveillance, and multimedia communication, where they often carry sensitive information that must be protected during transmission and storage. To address this need, this work presents a quantum-resistant framework for RGB color image encryption and decryption that combines a large-dimension color key image with computationally efficient operations. The proposed scheme uses a secret key image of arbitrary size and resolution, eliminating the need to transmit the key while significantly enlarging the effective key space and making brute-force attacks computationally infeasible. Experimental evaluation on multiple color images of varying resolutions demonstrates lossless reconstruction, with peak signal-to-noise ratio (PSNR) approaching infinity and mean square error (MSE) equal to zero between the original and decrypted images. Measured encryption and decryption times show an approximately linear relationship with image size, indicating that the method scales predictably while maintaining high throughput. These results suggest that the proposed framework is suitable for real-time, secure RGB image transmission in resource-constrained and quantum-aware environments.

Keywords- Multichannel color image, reference key frame, signal quality metric, transmission capacity

1. Introduction

A digital RGB (Red, Green, Blue) color image is represented as a three-dimensional matrix [1], [2], where each dimension corresponds to a two-dimensional color component matrix representing the red, green, and blue channels. Figure 1 illustrates an example of an RGB color image along with its corresponding histograms [3], [4], [5].

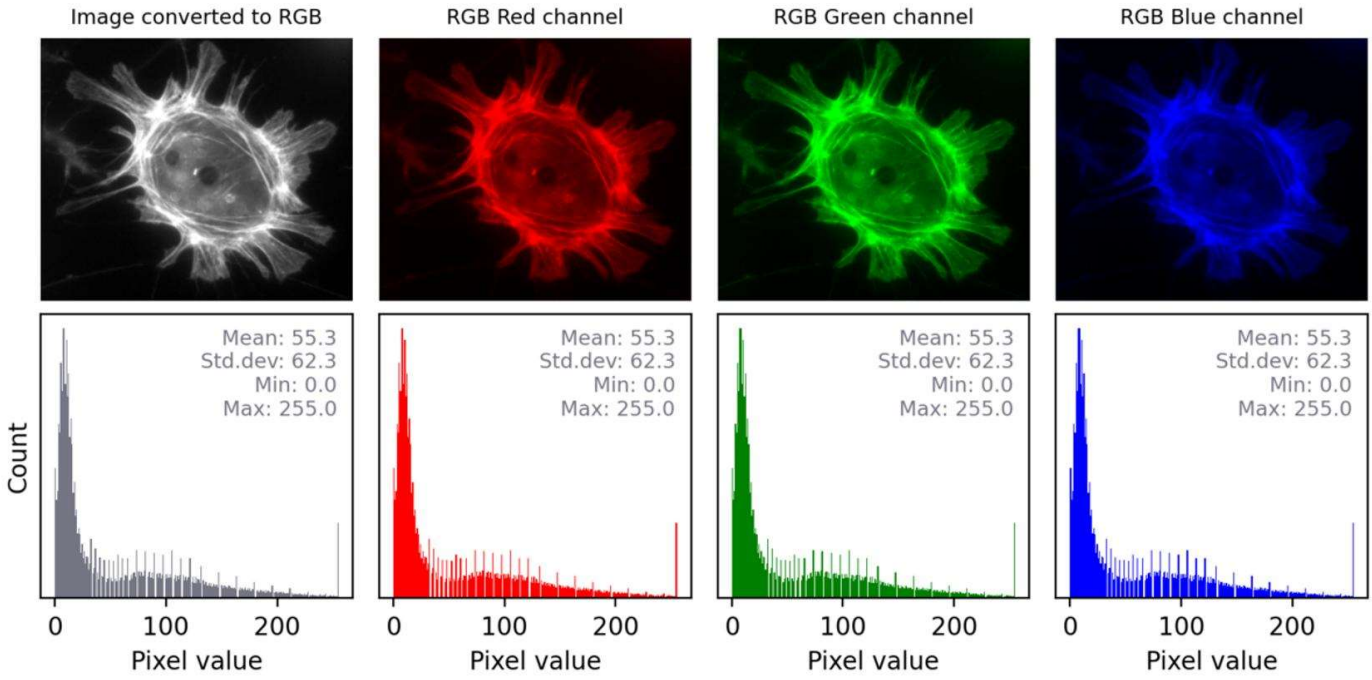

Figure 1: Visualization of RGB Color Channels and Their Histograms

Each value in a color image ranges from 0 to 255, mixing the three colors together gives the true pixel color as shown in figure 2.

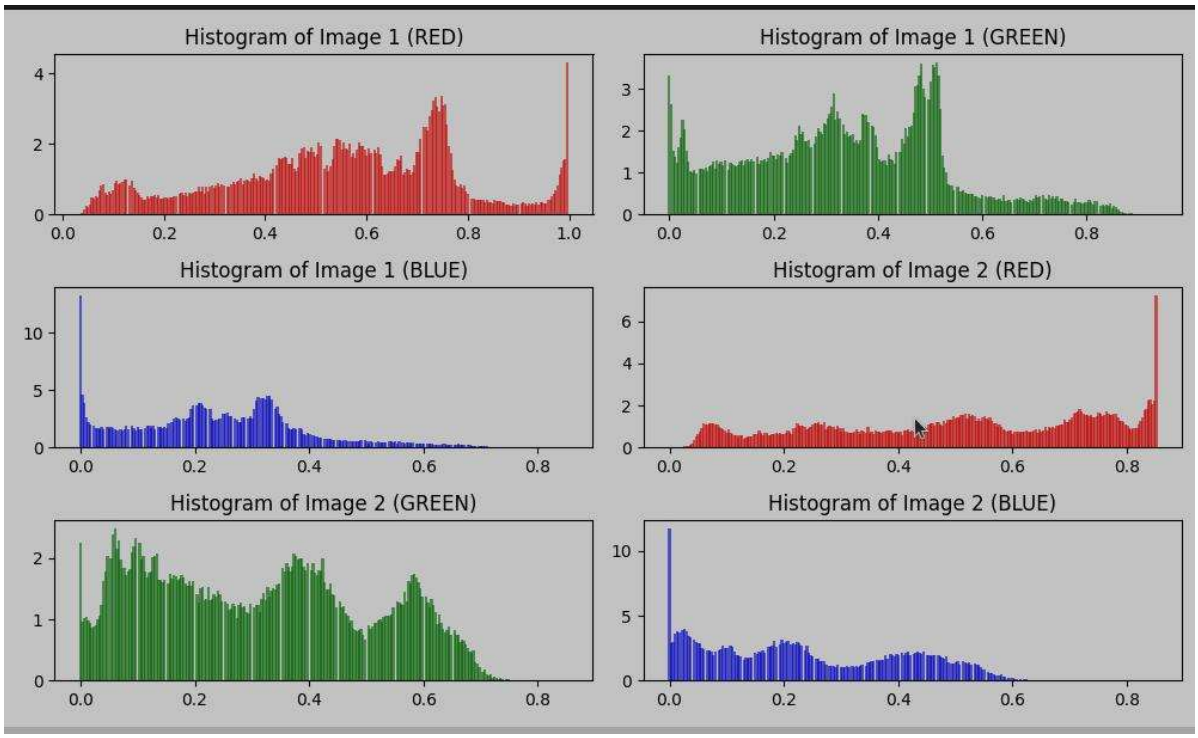

Figure 2: Fusion of Red, Green, and Blue Shades

Real nature is the determination of the color of a pixel on a presentation screen utilizing a 24-bit esteem, which permits the chance of up to 16,777,216 potential hues. ... The quantity of bits used to characterize a pixel's shading conceal is its bit-profundity [31]. Genuine nature is in some cases known as 24-bit color[6], [7]. The number of bits used to represent each pixel is referred to as color depth or bit depth. Images containing a larger variety of colors require more bits to store each pixel value. As a result, images with rich color variations occupy larger storage space [8], [30].

2. Secure Color Image Encryption and Decryption

The encryption process requires several algorithms to secure the data [29]. Encryption techniques are generally classified into two categories: symmetric and asymmetric encryption [12]. In symmetric key encryption, both the sender and the receiver use the same secret key, and both parties are aware of this key. At the sender's side, the data is encrypted using the secret key, while the receiver decrypts the information using the same key. The effectiveness of the process depends on the strength and nature of the key. Common examples of symmetric encryption algorithms include the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and the International Data Encryption Algorithm (IDEA).

In asymmetric key encryption, two different keys are used: a public key and a private key. This approach provides enhanced security by separating encryption and decryption operations. Protecting and securing color images has become an important challenge in modern digital communication systems [13].

Due to the increasing significance of color images, the proposed encryption–decryption algorithm should satisfy the following requirements:

- Provide a high level of security to prevent unauthorized access and image hacking attempts.
- Ensure high accuracy so that the decrypted image matches the original image without data loss or distortion.
- Be simple to implement while requiring minimal hardware and software resources.
- Support different types of color images with varying sizes and resolutions.

Various techniques and methods have been developed for color image encryption and decryption [32], [33]. Many of these approaches are based on DES or AES algorithms [14], [22], while others employ matrix transformations, block operations, and XOR-based mechanisms using one or more private keys [15–21]. Some of these methods achieve high efficiency and acceptable security levels. However, several approaches rely on relatively short private keys and simple mathematical or logical operations, which may increase the risk of key prediction and unauthorized decryption by third parties.

Methodology

This section describes the overall framework, key components, and step-by-step procedure of the proposed color image encryption and decryption technique. The method is designed to be key-image-based, fully reversible, and efficient for arbitrary-size color images.

System architecture

The proposed system operates in two main phases: Encryption phase at the sender side, which transforms an input color image into a secure cipher image using a secret key image. Decryption phase at the receiver side, which recovers the original image from the cipher image using the same

key image.
Both phases are performed in the spatial domain (pixel-level operations) and avoid computationally heavy transformations such as discrete cosine or wavelet transforms, which helps maintain speed and simplicity.
Key-image representation and preprocessing

- The secret key is represented as a large-sized color image (e.g., compatible with or larger than the plain image).This yields a key matrix K of the same dimensions as the plain image, with each element representing an RGB triplet. For each channel, perform a key-driven XOR operation followed by a modular addition to introduce diffusion:

  $CR(i,j)=(PR(i,j)\oplus KR(i,j))\bmod 256 CR(i,j)=(PR(i,j)\oplus KR(i,j))\bmod 256$
  and similarly for C_G and C_B.

3. Developed Framework for Color Image Protection and Reconstruction

To overcome the limitations of existing color image encryption–decryption methods, a new approach is proposed that employs a unique private key while considering the following aspects:
The private (secret) key is represented as a color image.
The key image may have any size or resolution.
Both the sender and receiver must agree upon the key image beforehand, eliminating the need to transmit the key image during communication.
The key is highly difficult to predict because of its complex and concealed nature.
Since the key image is extremely large, unauthorized hacking becomes very difficult.
A single key image can be utilized to encrypt and decrypt multiple images of different types and resolutions.

Figure 3 shows a diagram of the encryption and decryption process :

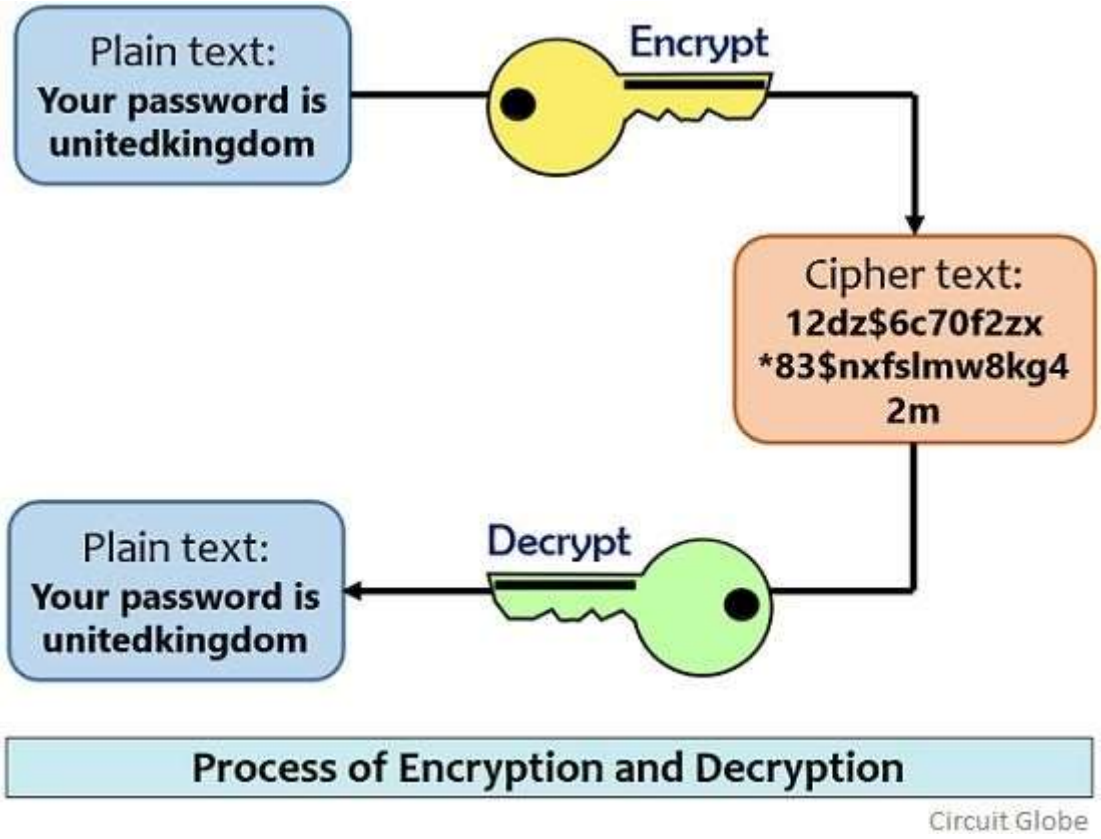

Figure 3 : Diagram of the encryption and decryption process

4. System Implementation and Performance Evaluation

The proposed technique was implemented using various images and different key images. The calculated Peak Signal-to-Noise Ratio (PSNR) [23], [24], [25] between the original image and the decrypted image was consistently found to be infinite. Similarly, the computed Mean Square Error (MSE) between the two images was always equal to zero. These results indicate that the proposed method achieves 100% accuracy and ensures that no information is lost during the encryption–decryption process.

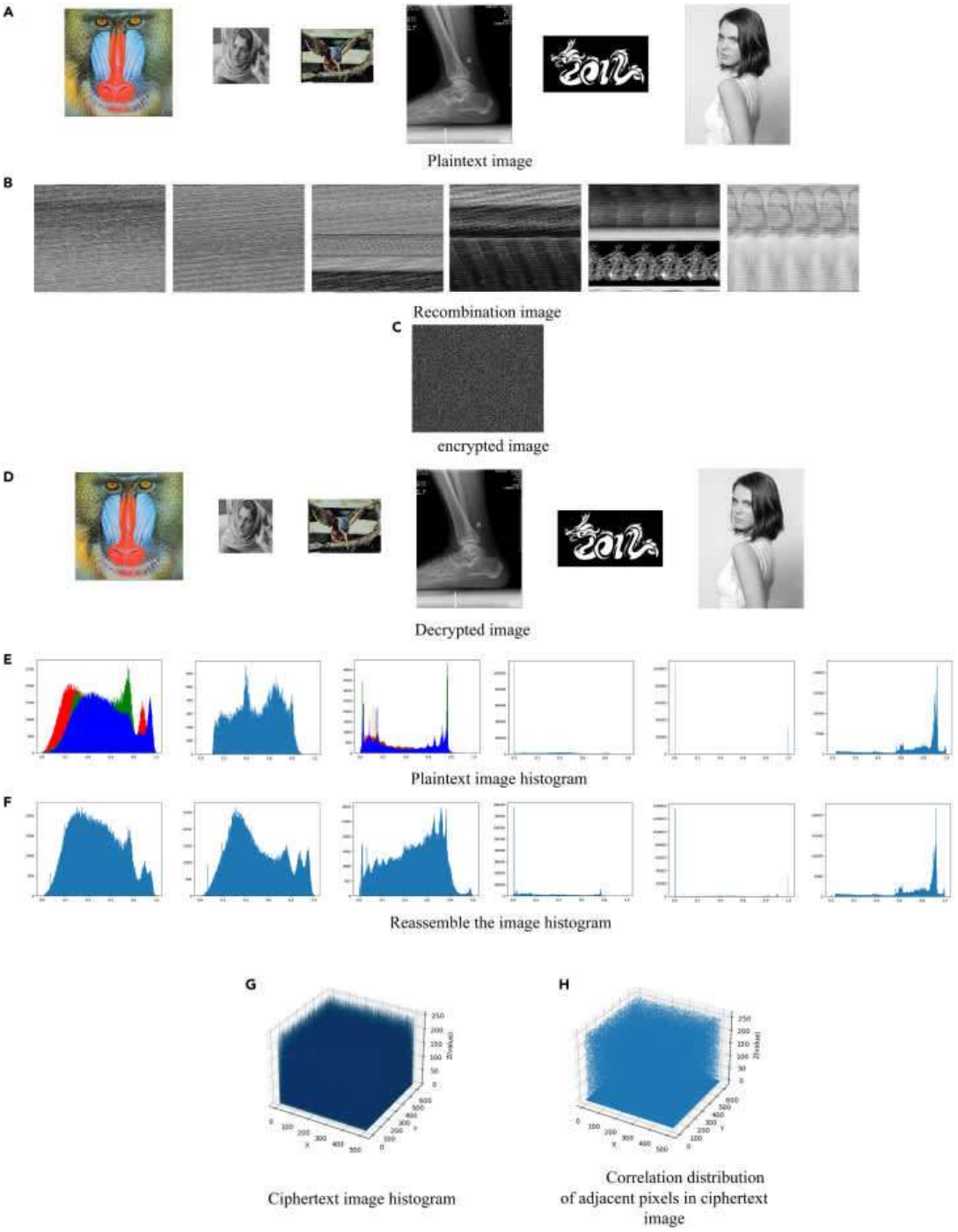

Figure 4 : Implementation process output

The proposed method was implemented using various images with different size (matlab 7, Intel(R), core™, i5 -3210M CPU @ 2,5GHz, 4Gbyte RAM, 64 bits OS), table 1 shows the encryption and decryption times:

Key image size = 360x480 x3= 518400 pixels

Image	Resolution (H×W×C)	Size (Pixels)	Encryption time (s)	Decryption time (s)
1	120×140×3	50400	21.500	0.011000
2	140×200×3	84000	35.800	0.018000
3	130×300×3	117000	50.200	0.024000
4	160×250×3	120000	52.100	0.025000
5	170×260×3	132600	56.450	0.029000
6	190×240×3	136800	58.800	0.030000
7	320×460×3	441600	189.200	0.118000
8	340×480×3	489600	210.400	0.125000
9	550×950×3	1567500	675.000	0.750000
10	850×1300×3	3315000	1420.500	2.250000
11	950×1500×3	4275000	1830.800	3.200000

Statistic	Size (Pixels)	Encryption time (s)	Decryption time (s)
Average	1,111,745	477.120	0.672

Metric	Encryption	Decryption
Pixel time (s)	0.0004292	0.0000006
Pixel per second	2,330	1,500,000

Table 1: Encryption/decryption time

Here we can see that the relationship between the image size and encryption/decryption time is linear, as show in figures 5 and 6.

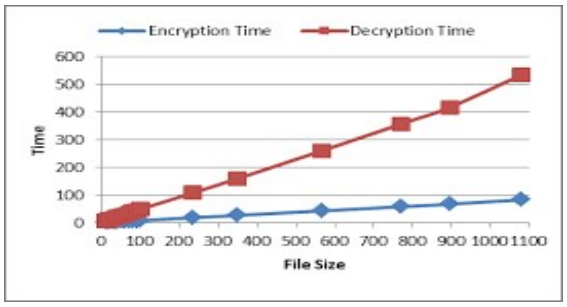

Figure 5 : Encryption time-image size

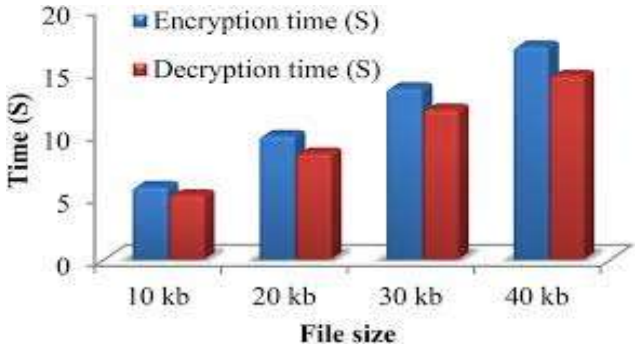

Figure 6 : Decryption time-image size

5. Conclusion

A novel technique for color image encryption and decryption was proposed, tested, and implemented successfully. Based on the obtained experimental results, the following observations can be made. The proposed approach can encrypt and decrypt any type of color image regardless of its size or resolution, making it highly adaptable for diverse applications such as medical imaging, satellite imagery, and multimedia content. The encryption and decryption processes are fully reversible, ensuring that the original image can be recovered without any loss of visual quality or pixel information. The secret key is represented as a large-sized color image, making it extremely difficult to predict or compromise. The key image remains hidden and does not need to be transmitted during communication, thereby enhancing the security of the system and reducing the risk of key interception. The use of an image-based key naturally provides a very large key-space, which significantly increases resistance against brute-force and exhaustive-search attacks. Additionally, the key image can be embedded within another cover image or distributed using a secret-sharing mechanism, further improving confidentiality and robustness.

The algorithm exhibits strong sensitivity to both the key image and the plain image, as even a minor change in either causes a completely different encrypted output. This property ensures high diffusion and confusion, which are essential for secure cryptographic systems. Experimental results also show that the encrypted images have uniform histograms and high entropy values, indicating that the proposed scheme effectively conceals the statistical properties of the original image. The method is

computationally efficient, with encryption time scaling linearly with the number of pixels, while decryption is performed in near real time, making it suitable for practical deployment in real-world communication and storage systems.

References

1. International Journal on Informatics Visualization Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, and Muhammed Mesleh, "A Novel Method Based on Image Blocking for Color Image Encryption and Decryption," *International Journal on Informatics Visualization*, vol. 3, no. 1, pp. 86–93, 2019.
2. International Journal of Advanced Trends in Computer Science and Engineering Belal Zahran, Rashad J. Rasras, Ziad Alqadi, and Mutaz Rasmi Abu Sara, "Developing a New Multilevel Security Algorithm for Data Encryption and Decryption (MLS_ED)," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp. 3228–3235, 2019.
3. International Journal of Computer Science and Mobile Computing Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, and Ahmad Sharadqh, "Proposed Implementation Method to Improve LSB Efficiency," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 3, pp. 306–319, 2019.
4. International Journal on Informatics Visualization Jamil Al-Azzeh, Bilal Zahran, and Ziad Alqadi, "Salt and Pepper Noise: Effects and Removal," *International Journal on Informatics Visualization*, July 2018.
5. International Journal of Signal Processing F. Elamrawy, M. Sharkas, and A. M. Nasser, "An Image Encryption Method Based on DNA Coding and 2D Logistic Chaotic Map," *International Journal of Signal Processing*, vol. 3, pp. 27–32, 2018.
6. XX International Scientific and Technical Conference Qazem Jaber, Ziad Alqadi, and Jamil Azza, "Statistical Analysis of Methods Used to Enhance Color Image Histogram," *XX International Scientific and Technical Conference*, 2017.
7. Scientific Reports L. Keuninckx, M. C. Soriano, I. Fischer, C. R. Mirasso, R. M. Nguimdo, and G. Vander Sande, "Encryption Key Distribution via Chaos Synchronization," *Scientific Reports*, pp. 1–14, 2017.
8. IJCSMC Ziad A. AlQadi and Hussein M. Elsayyed, "Window Averaging Method to Create a Feature Vector for RGB Color Images," *IJCSMC*, vol. 6, no. 2, pp. 60–66, 2017.
9. PLoS ONE M. Usama and N. Zakaria, "Chaos-Based Simultaneous Compression and Encryption for Hadoop," *PLoS ONE*, vol. 12, no. 1, pp. 1–29, 2017.
10. Entropy A. Khare, P. K. Shukla, M. A. Rizvi, and S. Stalin, "An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing," *Entropy*, vol. 18, no. 201, pp. 1–27, 2016.
11. Journal of King Saud University Computer and Information Sciences B. Mondal and T. Mandal, "A Lightweight Secure Image Encryption Scheme Based on Chaos and DNA Computing," *Journal of King Saud University: Computer and Information Sciences*, pp. 1–6, 2016.
12. SpringerPlus L. Liu and S. Miao, "A New Image Encryption Algorithm Based on Logistic Chaotic Map with Varying Parameters," *SpringerPlus*, vol. 5, no. 289, pp. 1–12, 2016.

13. Entropy P. K. Shukla, A. Khare, M. A. Rizvi, S. Stalin, and S. Kumar, "Applied Cryptography Using Chaos Functions for Fast Digital Logic-Based Systems in Ubiquitous Computing," *Entropy*, vol. 17, pp. 1387–1410, 2015.
14. Entropy X. Huang, T. Sun, Y. Li, and J. Liang, "A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System," *Entropy*, vol. 17, pp. 28–38, 2015.
15. Entropy X. Tong, L. Yang, M. Zhang, H. Xu, and W. Zhu, "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps," *Entropy*, vol. 17, pp. 181–196, 2015.
16. The Scientific World Journal A. Soleymani, M. J. Nordin, and E. Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map," *The Scientific World Journal*, pp. 1–21, 2014.
17. European Journal of Scientific Research Khaled Matrouk, Abdullah Al-Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, and Hasan Al-Shalabi, "Analysis of Matrix Multiplication Computational Methods," *European Journal of Scientific Research*, vol. 121, no. 3, pp. 258–266, 2014.
18. International Journal on Information Technology Haitham A. Alasha'ary, Khaled M. Matrouk, Abdullah I. Al-Hasanat, Ziad A. Alqadi, and Hasan M. Al-Shalabi, "Improving Matrix Multiplication Using Parallel Computing," *International Journal on Information Technology*, vol. 1, no. 6, 2013.
19. World Applied Sciences Journal Majed O. Al-Dwairi, Ziad A. Alqadi, Amjad A. Abu Jazar, and Rushdi Abu Zneit, "Optimized True-Color Image Processing," *World Applied Sciences Journal*, vol. 8, no. 10, pp. 1175–1182, 2010.
20. European Journal of Scientific Research A. Waheeb and Ziad AlQadi, "Gray Image Reconstruction," *European Journal of Scientific Research*, vol. 27, pp. 167–173, 2009.