Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18722-x

An innovative image encryption algorithm enhanced with the Pan-Tompkins Algorithm for optimal security

Ayşegül İhsan[1] · **Nurettin Doğan**[2]

Received: 9 September 2023 / Revised: 19 February 2024 / Accepted: 23 February 2024
© The Author(s) 2024

Abstract

This study introduces a cutting-edge image encryption algorithm aimed at elevating security standards. The Pan-Tompkins Algorithm (PTA) for key generation is proposed for the first time in this study. Additionally, employing steganography through the Least Significant Bit (LSB) method for embedding keys within the encrypted image enhances secure key distribution, thereby fortifying the encryption process. On the other hand, the integration of advanced algorithms, such as Zigzag scanning, the Affine Image Encryption Algorithm (AA), and the Vigenere Image Encryption Algorithm (VA), constitutes the fundamental innovation of the proposed image encryption algorithm. The proposed algorithm is named PanAAVA:Affine Algorithm and Vigenere Algorithm Encryption with PTA-Based Key Generation. The PanAAVA algorithm ensures unparalleled security by encrypting the positions and values of pixels using AA and VA. Notably, using PTA for key generation marks a distinctive and new key generation method feature of the algorithm. To assess the effectiveness of the PanAAVA, a comprehensive comparative analysis is conducted against well-established encryption methodologies, including Lena, Baboon, Airplane, and Pepper. The PanAAVA demonstrates exceptional proficiency in histogram analysis. The PanAAVA demonstrates a Unified Average Changing Intensity (UACI) of 33.4044%. Additionally, the Number of Pixels Change Rate (NPCR) is measured at 99.7442%, showcasing the algorithm's effectiveness in inducing significant pixel changes. The proposed algorithm's Mean Square Error (MSE) is calculated at 3.20679E5%. The proposed algorithm's Peak Signal to Noise Ratio (PSNR) is recorded at 9.512475. The Key Space Size of the proposed algorithm is measured at 2^{209}. Regarding correlation analysis, the PanAAVA achieves a high correlation score of 7.9996. The proposed algorithm successfully passes the National Institute of Standards and Technology (NIST) analysis, demonstrating a remarkably strong correlation close to 0 and a Structural Similarity Index Measure (SSIM) of 0.9977. Furthermore, regarding quantum communication, the proposed algorithm maintains stable key rates of 47.5 ± 0.8 kHz during the day and 50.9 ± 0.7 kHz at night. Additionally, PanAAVA achieves low Quantum Bit Error Rate (QBER) values of 4.77 ± 0.02, ensuring reliable and secure communication. The PanAAVA also demonstrates robust asymmetries at 49.81 ± 0.02 and 50.14 ± 0.03 for a crystal length of 20 mm. highlighting PanAAVA's adaptability and effectiveness in different scenarios. PanAAVA outperforms other encryption algorithms concerning performance measurements and comparisons. In conclusion, the PanAAVA emerges as a beacon of superior security capabilities and innovation in image encryption, showcasing the potential to redefine standards in the field.

Extended author information available on the last page of the article

Published online: 14 March 2024

Keywords Affine · Image Encryption · Key Generation · Pan-Tompkins Algorithm · R-peak · Least Significant Bit (LSB) · Vigenere

1 Introduction

Amidst the rapid evolution of the digital landscape, safeguarding digital images has emerged as an imperative task. In today's interconnected world, where technology pervades every facet of life and industries rely heavily on digital data, ensuring the security of digital assets, especially images, has become increasingly crucial. As businesses and organizations pivot towards digital solutions and embrace digital communication channels, the need for secure data transmission has become more pronounced than ever before [1, 2]. This study introduces an advanced image encryption algorithm meticulously designed to address existing limitations, specifically focusing on pixel location and value preservation. The proposed algorithm is named PanAAVA:Affine Algorithm and Vigenere Algorithm Encryption with PTA-Based Key Generation. Positioned as a pioneering response to the escalating challenges in information security, particularly in image encryption, the PanAAVA seeks to bridge critical gaps in security practices and set new standards for encryption in the digital realm. The characterization of optimal security underscores a steadfast commitment to achieving the highest security standards, particularly in safeguarding sensitive digital data across diverse industry sectors. The successful journey of the recommended algorithm through in-depth study reveals the capabilities to overcome existing limitations and elevate security standards, particularly within various industry sectors.

By integrating advanced methods and algorithms such as the Pan-Tompkins Algorithm (PTA), Zigzag scanning, the Affine Image Encryption Algorithm (AA), and the Vigenere Image Encryption Algorithm (VA), this algorithm is designed to be versatile and applicable across various. Leveraging PTA for key generation and incorporating the Least Significant Bit (LSB) stenography method enhance security effectiveness, minimize visual distortion, and streamline secure key distribution processes.

This study meticulously identifies fundamental limitations in prevailing encryption methodologies and proposes effective solutions through a comprehensive analysis tailored to the specific security needs of industry applications. The successful journey of the recommended algorithm through in-depth scrutiny underscores the ability to overcome existing limitations and elevate security standards, particularly within various industry sectors. In essence, the significant advantages of the new algorithm, showcasing the pioneering effect in overcoming the limitations of current encryption approaches, are summarized as follows:

- Current encryption methods and algorithms often require improvements, particularly in preserving the integrity of pixel positions and values throughout the encryption process. This study introduces an innovative image encryption algorithm that offers enhanced effectiveness and security to address the limitations observed in the PanAAVA.
- The primary focus of this proposed encryption algorithm centers on presenting an innovative image encryption algorithm that seamlessly integrates advanced methods and algorithms, including Zigzag scanning, AA, VA, and LSB.
- Furthermore, the PTA is utilized for key generation for the first time in the literature. Steganography is introduced to the image encryption algorithm by incorporating LSB and keys into the image. This enhancement results in a more robust encryption.

- The meticulous presentation and comparison of all encryption results and thorough analysis contribute to establishing a robust security representation for the algorithm. Undoubtedly, this study positions the proposed algorithm as a trailblazer, revealing distinctive and optimal security capabilities and innovations in image encryption.
- Additionally, PanAAVA is designed to be compatible with quantum computing systems. Therefore, the potential of PanAAVA for significant future developments in quantum computing is demonstrated.

The study unfolds in several sections. Section II presents a literature review. Section III provides a concise overview of essential methodologies, including AA, VA, LSB, PTA for R-Peak Detection, and Zigzag scanning, setting the foundation for the encryption algorithm. Section IV delves into a comprehensive explanation of the proposed encryption algorithm. The PanAAVA's performance is scrutinized in Section V, evaluating the effectiveness across diverse color images in terms of security and efficiency. Section VI examines the test results, discusses potential impacts and applications, and emphasizes the algorithm's contribution to the advancement of image encryption. The study concludes by summarizing the findings and providing observations in the final section.

2 Literature review

The burgeoning importance of security in digital environments catalyzed the evolution of various techniques, prominently featuring pixel permutation, pixel substitution, and image encryption employing Gray code. Notably, a noteworthy advancement in encryption algorithms elevated the role of the Affine Image Encryption Algorithm (AA) by seamlessly integrated Gray code-based bit-plane analysis with the pixel permutation methodology, thereby highlighting the pivotal role of AA in shaping and fortifying encryption strategies [3]. In hyperspectral data encryption, an innovative approach was devised utilizing the Fractional Fourier Transform (FrFT) framework. This method entailed segmenting data into bands, applying AA, and encrypting within the FrFT domain, leveraging AA and FrFT parameters to ensure security in both spatial and spectral data [4]. Several encryption algorithms were introduced, including the Random Matrix Affine Algorithm (RMAA), 2-dimensional Fractional Hartley Transform (RP2D-FrHT), and 2-dimensional Arnold maps. RMAA enhanced security in coordinate and geometric domains, while RP2DFrHT simplified complexity, yielding digitally suitable real-valued encrypted data. Integration of the 2D Arnold map further fortified security and expanded the key space [5]. Another significant contribution was the Improved Affine Algorithm (IAA), which combined AA, Linear Feedback Shift Register (LFSR), and XOR encryption algorithm [6]. Additionally, a color image encryption algorithm incorporated a 2D Hénon map, a three-dimensional logistic map with XOR operation, and AA augmented system security [7]. Further diversification was evident in a hybrid image encryption algorithm, amalgamating traditional methods with an extended-dimensional chaotic map, enhancing security measures. Comparative analysis of optimization results for transposition methods against classical algorithms yielded improved image encryption outcomes [8]. Improved VA schemes and chaotic permutations were explored in various studies to address recurring key issues and develop innovative password-strengthening strategies [9]. One study combined VA with Huffman Encryption to devise a robust encryption algorithm, segment images into blocks, and intricately embed data in pixel group [10]. Real-time image encryption employed modified VA and chaotic maps to extend 8-tuple keys to 8×8 blocks, encrypting pixel blocks through XOR operations, Arnold transformations, and Baker maps [11]. Another encryption algorithm for RGB images used unique S-box arrangements over a Galois field, while AA scrambled image data, further strengthening security [12]. A novel image encryption algorithm was introduced in this study, utilizing the improved the VA alongside LSB method [13]. Another study proposed a hybrid method derived from VA and Beaufort cipher algorithm modifications. This method utilized two random keys: one composed of 8-bit integer values and the other consisting of binary values [14]. As proposed in another study, the algorithm significantly improved traditional VA encryption by two steps. Leveraging advanced dynamic permutation matrices and chaotic maps established robust encryption [15]. In another study, the combined usage of Hash Least Significant Bit (H-LSB) and VA methods was proposed to enhance image security. Additionally, a system incorporating a multi-layered security technique utilizing steganography was suggested [16]. In the literature review focusing on Zigzag scan, a color image encryption algorithm was developed using a CNN chaotic system. The algorithm introduced randomness by utilizing encrypted key matrices generated with LFSR. Combining DNA encoding, bit-plane decomposition, and high-bit-plane Zigzag scan achieved robust security [17]. The proposed alternative algorithm facilitated image encryption using a complex, chaotic system and changed pixel positions through the zigzag scan. The robust ergodicity, complex, chaotic behavior, and stable Lyapunov exponential spectrum inherent in the chaotic system presented [18]. Upon scrutiny of LSB literature, an alternative algorithm was proposed, amalgamating Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and LSB methodologies [19]. A dual-layered approach was employed in a separate study, initially encoding a digital image using LSB steganography, followed by an extra layer of security through AES encryption [20]. Furthermore, a study focused on enhancing data transmission speed by selectively encrypting bits in the Triple Data Encryption Standard (T-DES), ensuring security and performance [21]. The recent studies in image encryption are summarized in Table 1.

3 Background

This section examines The Affine Image Encryption Algorithm (AA), The Vigenere Image Encryption Algorithm (VA), Least Significant Bit (LSB) embedding, the Electrocardiogram and the Pan-Tompkins Algorithm (PTA) for R-Peak Detection, and the Zigzag scan.

Table 1 Some recently developed image encryption algorithms

Year	Recently developed image encryption algorithm	
2024	Simultaneous Chaotic Image Encryption	[22]
2024	Color Image Encryption Algorithm based on Improved One-Dimensional Chaotic Map	[23]
2024	Quantum Chaotic Map and DNA Coding based Image Encryption Algorithm	[24]
2024	Plaintext Sensitive Chaotic Image Encryption Algorithm	[25]
2024	Bessel Map based Image Encryption	[26]

3.1 Affine image encryption algorithm

The Affine Image Encryption Algorithm (AA) is utilized for plaintext encryption, altering pixel values and pixel locations within the image [27]. Equation 1 utilizes the AA to encrypt each pixel in the image.

$$C = (a \times p + b) \bmod 256,\ 0 \le p \le 255 \tag{1}$$

where C represents the encrypted pixel value, p denotes the original image's pixel, and a and b are the encryption keys. The value 256 signifies the maximum of a pixel in an 8-bit grayscale image. The decryption process employs the subsequent formulas:

$$p = \overline{a} \times (c - b) \bmod 256,\ 0 \le p \le 255 \tag{2}$$

$$\overline{a} \equiv a^{\varphi(256)-1} \bmod 256 \tag{3}$$

where $\overline{a}$ represents the modular multiplicative inverse of a modulo 256, to compute the modular inverse of a modulo 256, Euler's totient function, designated as φ(256), is employed. φ(256) provides the count of positive integers less than 256 that are coprime with 256. In simpler terms, p determines the number of integers between 0 and 255, not share any common factors with 256 [28]. Euler's totient function for 256, φ(256). The modular inverse of a concerning 256 is determined by raising a to the power of φ(256)-1 and subsequently taking the modulus 256 of the result.

3.2 The vigenere image encryption algorithm

The Vigenere Image Encryption Algorithm (VA) is a polyalphabetic cipher used for encryption. VA employs a tabular form, the VA table, consisting of elements. The first row contains n different elements, while subsequent rows are formed by left cycle shifting of the elements from the previous row. Decryption involves looking up the ciphered element in the row corresponding to the key element, with the column representing the decrypted output or the original letter. Originally developed for encrypting alphabetical texts, recent studies have adapted the VA concepts for image encryption [29]. The VA encryption and decryption of an image matrix of order 2^N. The encryption equation used in the VA is as follows:

$$a(\mathrm{M}, \mathrm{K}) = \mathrm{C} = \mathrm{M} + \mathrm{K} \bmod 2^{\mathrm{n}} = \left[\mathrm{m}_{\mathrm{ij}} + \mathrm{k}_{\mathrm{ij}}\right](\bmod 2^{\mathrm{n}}) \tag{4}$$

where a represents the encryption image, i and j denote the image block's i-th row and j -th column, M and $[\mathrm{m}_{\mathrm{ij}}]$ represent the original image matrix, K and $[\mathrm{k}_{\mathrm{ij}}]$ represent the key matrix, C and $[\mathrm{c}_{\mathrm{ij}}]$ denote the encryption matrix, with c_{ij} representing elements, and 2^{N} refers to the size matrix. Equation 5 is used for decryption by the VA.

$$\overline{a}(C, K) = M = C - K \bmod 2^n = \left[c_{ij} - k_{ij}\right](\bmod 2^n) = \left[c_{ij} + 2^n - k_{ij}\right](\bmod 2^n) \tag{5}$$

where $\overline{a}$ represents the decryption image, n is a positive integer [11].

3.3 Least significant bit steganography

Steganography, an ancient method dating back to ancient Greece, involves concealing information within digital media while preserving the overt characteristics of the media. Typically, steganography uses a cover image and a hidden message, creating a stego image. One common method, Least Significant Bit (LSB) insertion, alters pixel values to hide the embedded message [30]. The length of the encryption key plays a critical role in ensuring security, with longer keys providing greater protection. In this process, the key encrypts the message, and the encrypted key is subtly incorporated into the RGB values of the cover image using LSB steganography. This method ensures that the alterations are imperceptible, making detection challenging. Only authorized recipients possessing the decryption key can extract the hidden message, ensuring high levels of security and confidentiality. The encryption key is indispensable in LSB steganography, guaranteeing the confidentiality and security of the transmitted message. During the embedding process, message bits replace the LSBs of pixels, randomly or sequentially selected from the cover image [31]. Equation 6 elucidates the method of utilizing LSB to embed data.

$$y_i = 2\left(\frac{\mathrm{x}_i}{2}\right) + \mathrm{m}_i \tag{6}$$

where x_i and y_i are the i-th chosen pixel values before and after embedding, and m_i stands for the i-th message bit.

3.4 The electrocardiogram and The Pan-Tompkins Algorithm for R-Peak detection

The Electrocardiogram (ECG) is a fundamental tool in monitoring cardiac health, capturing the heart's electrical activity through a waveform consisting of key components like the P wave, QRS complex, and T wave. The QRS complex holds particular significance among these components, representing ventricular depolarization events. To precisely detect QRS complexes and identify R-wave peaks, crucial in clinical diagnosis, the Pan-Tompkins Algorithm (PTA) emerges as a pivotal solution. Tailored for ECG signal analysis, PTA employs a series of filters to enhance statistical characteristics and minimize noise, facilitating accurate interpretation of ECG data [32]. The PTA is widely used for detecting R-peaks in ECG signals. The PTA consists of several stages:

1. Band-pass Filtering: The ECG signal is initially filtered using a band-pass filter to remove unwanted noise and interference while preserving the essential components of the signal within the frequency range associated with the QRS complex.
2. Differentiation: Following filtration, the signal undergoes differentiation to amplify the steep slope characteristic of the QRS complex. This process enhances the detection of rapid voltage changes associated with the depolarization of the ventricles.
3. Squaring: The squared signal is computed to accentuate the amplitude of the QRS complex. Squaring the signal emphasizes the high-energy components of the QRS complex. This stage aims to increase the distinguishability of the QRS complex from other components present in the ECG waveform.
4. Integration: The squared signal undergoes integration over a specified window to obtain an average value. Integration smooths out the signal and highlights the areas with sustained high energy, such as the QRS complex.

5. Thresholding: A threshold is established to distinguish QRS complexes from background noise. Signals exceeding this threshold are identified as potential QRS complexes, with the R-peak being the highest point within each complex.
6. Refractory Period: A refractory period is implemented to prevent the detection of multiple R-peaks within a brief time interval. Additional R-peaks are ignored during this period, ensuring that only the most prominent peak is detected.

In summary, the PTA serves as a pivotal tool in precisely identifying QRS complexes, especially R-wave peaks, within ECG signals.

3.5 Zigzag scan

The Zigzag scan, recognized for the contribution to enhanced compression and transmission efficiency in image and video processing, extends the significance into image encryption, a pivotal component in safeguarding sensitive content. While the primary role is to optimize compression and transmission, including image encryption introduces an additional layer of complexity, making it challenging for unauthorized individuals to decrypt images and access confidential information [33].

A Zigzag scan is a process whereby the elements of an image are sequentially scanned in a specific pattern during processing. This method contributes to the efficient utilization of processing resources by enabling effective handling of image data. The process of performing parallel zigzags from top to bottom and right to left involves representing the image in matrix form. Subsequently, the elements of this matrix are processed sequentially following a predetermined zigzag pattern. Executing this process in parallel involves simultaneously processing different segments using multiple processing units or parallel processing techniques. Such an approach reduces processing time while optimizing processing power usage. The zigzag scan is commonly favored in fields such as image processing, video coding, and related domains.

4 Proposed algorithm

The intricately designed PanAAVA consists of five stages, each meticulously crafted to fulfill a specific purpose aimed at robust and secure image encryption. PTA takes center stage in the initial phase by expertly identifying R-peaks within an ECG signal. These identified points form the basis for generating unique and random cryptographic keys, paving the way for subsequent encryption processes. This innovative approach provides a durable foundation for the security architecture of the algorithm, enabling the derivation of highly secure keys. In the second stage, the RGB layers of the image are passed through a meticulous Zigzag scanning process. Characterized by sophistication, this step not only increases the efficiency of encryption and decryption but also significantly increases the overall security and usability of the algorithm. In the third and fourth stages of the algorithm, AA and VA-based encryption algorithms are introduced, respectively. The fifth and final stage of the algorithm involves inserting the keys obtained from R-peak detection into the encrypted image using the LSB method. Figures 1 and 2 provide a comprehensive overview of the algorithmic steps by providing understandable visual representations of the encryption and decryption processes. The PanAAVA is a testament to the effectiveness of combining innovation with security in various applications.

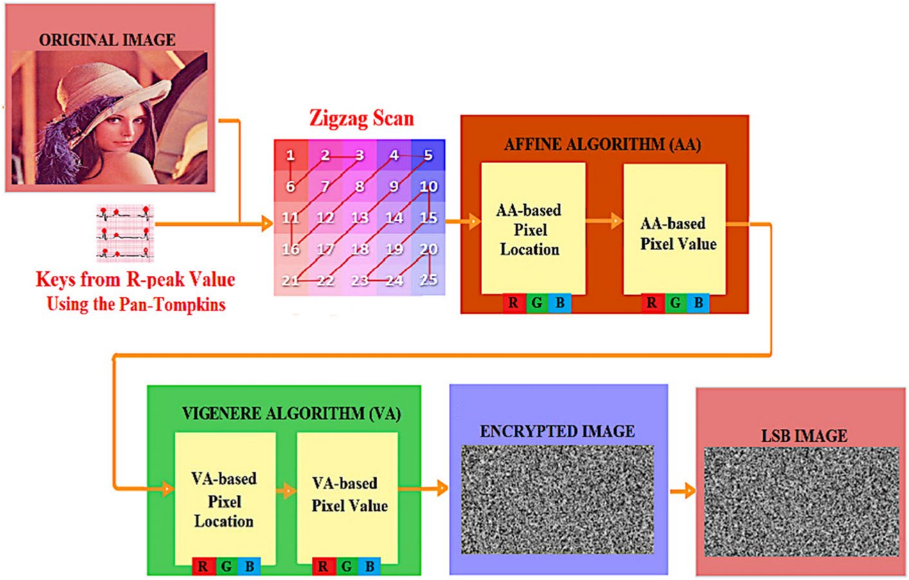

Fig. 1 The block diagram of the PanAAVA

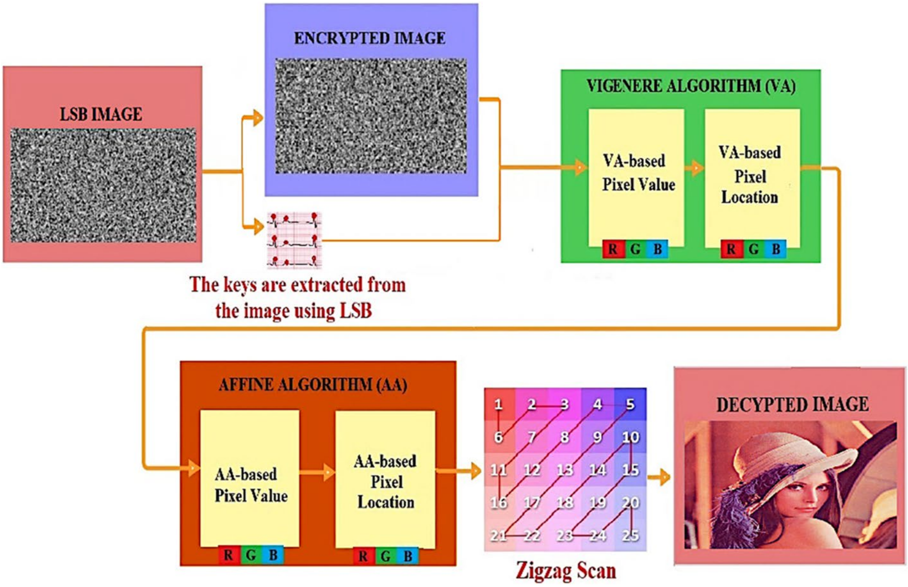

Fig. 2 The block diagram of the PanAAVA

(i) Generation of the Proposed Algorithm's Keys

In this study, the PTA is specifically chosen for ECG data due to the proposed algorithm's unparalleled accuracy in QRS detection, robustness against noise, real-time processing capabilities, documented success in medical applications, simplicity, computational efficiency, and adaptability to signal nuances. PTA's flexibility in processing a variety of signal sources, together with PanAAVA's proven effectiveness in extracting necessary information from ECG data, highlights the algorithm's applicability in a wide range of scenarios. This study utilizes the PTA to generate image encryption keys in a proposed algorithm by leveraging an ECG-based key dataset. With the precision of the PTA, 256 unique R-peak positions are extracted and seamlessly integrated as encryption keys into the AA and VA for a selected image. This integration represents a significant advancement in image encryption algorithms. The PanAAVA effectively secures sensitive image data while preserving image quality, offering a robust and effective solution for image encryption.

(ii) Zigzag Scan

The PanAAVA elevates the security of color image encryption by integrating a Zigzag scan, a pivotal step that significantly enhances the encryption process. The algorithm ensures comprehensive coverage and robust image data protection through individual scanning of the RGB layers. The algorithm generates input data for the subsequent encryption phases meticulously outlined by applying the Zigzag scan to the original image. This multifaceted encryption PanAAVA encompasses Zigzag scanning, pixel location, and pixel value encryption, each contributing to the overall security framework. By incorporating diverse methods and different algorithms, the proposed algorithm fortifies defenses against potential threats, ensuring the utmost confidentiality and integrity of the encrypted image data.

(iii) AA-based Pixel Value and Location Encryption with R-peak Value Key

The AA encryption in the PanAAVA ensures robust image security through a two-step process. Initially, RGB layers are independently encrypted for pixel locations using key sets (a_1, b_1) and (a_2, b_2), thereby adding an extra layer of security. In the subsequent stage, pixel values are encrypted using six unique keys: (a_3, b_3), (a_4, b_4), (a_5, b_5). This process significantly increases decryption complexity, providing a strong defense. The initial 10 distinct 256 keys derived from the ECG signal R-peaks for AA encryption are strategically selected. This approach maintains complexity and reliability while minimizing computational and storage requirements. Incorporating the 10 distinct 256 keys derived from the ECG signal's R-peaks for AA encryption is pivotal, enhancing both effectiveness and efficiency and rendering the algorithm ideal for applications necessitating critical image security.

(iv) VA-based Pixel Value and Pixel Location Encryption with R-peak Value Key

256 keys derived from the ECG signal's R-peaks, both pixel locations and values undergo encryption, significantly bolstering the algorithm's security. The utilization of the R-peak value key for VA-based encryption introduces a level of unpredictability and complexity crucial for applications emphasizing image security. The choice to utilize 256 encryption keys, an additional layer of security, is introduced through VA-based encryption. Employing the PTA is strategic, as employing the PTA establishes a vast key space that effectively thwarts brute force attacks and ensures robust protection for encrypted data. This decision adheres to industry standards, as 256-bit encryption is widely acknowledged for robust security features. The selected key length creates a computationally infeasible environment for attackers attempting brute-force attacks. Consequently, opting for 256 encryption keys enhances the overall security posture of the algorithm, providing a high level of protection against potential threats and vulnerabilities for the encrypted data.

(v) Key Steganography with LSB

In the culminating step of the proposed algorithm, paramount attention is directed towards the secure embedding of keys, a critical element ensuring the confidentiality and reliability of the transfer process. The PanAAVA employs Eq. 5 as a foundational framework, leveraging a sophisticated stenographic approach with the LSB to integrate 256 distinct keys seamlessly. This advanced method provides a robust and highly effective means of concealing cryptographic keys within the fabric of images, ensuring the utmost level of security. Integrating steganography with the LSB method renders the embedded keys virtually indiscernible, thereby fortifying the concealment against potential intruders.

Figure 3 provides a comprehensive visual representation of the pseudo-code encapsulating the intricacies of the proposed algorithm. The utilization of steganography, particularly through LSB manipulation, underscores the algorithm's commitment to encryption and the covert integration of keys, enhancing the overall security posture against adversarial threats.

5 Results and performance analysis of the proposed algorithm

This study implemented the PanAAVA using the MATLAB 2022(a) programming language. Encryption keys are found by utilizing the PTA to find the R-peak locations of the ECG images from a large dataset. This dataset, compiled from the Ch. Pervaiz

Generation of Keys Based on PTA:
1. *Leveraging the Pan-Tompkins Algorithm (PTA), extract 256 unique R-peak positions from an ECG signal.*

Zigzag Scanning for Image Encryption:
1. *A Zigzag scan is applied to a color image, individually scanning RGB layers.*
2. *The resulting data from the Zigzag scan becomes the input for subsequent encryption steps, encompassing Zigzag scanning, pixel location encryption, and pixel value encryption.*

AA-based Pixel Value and Location Encryption with R-peak Value Key:
1. *RGB layers are independently encrypted for pixel locations using key sets* (a_1 , b_1) *and* (a_2 , b_2), *adding an extra layer of security.*
2. *Pixel values undergo encryption using six unique keys:* (a_3 , b_3), (a_4 , b_4), (a_5 , b_5), *significantly increasing decryption complexity.*

VA-based Pixel Value and Pixel Location Encryption with R-peak Value Key:
1. *Following AA encryption, an additional layer of security is introduced through VA-based encryption using 256 keys generated from R peaks.*
2. *Pixel locations and values are encrypted, strengthening the algorithm's security.*

Key Steganography with LSB for Secure Integration:
1. *In the final stage, 256 unique keys are discreetly integrated into the image using LSB steganography.*

Fig. 3 The decryption block diagram of the PanAAVA

Elahi Institute of Cardiology in Multan, Pakistan, is publicly accessible through this link: (https://data.mendeley.com/datasets/gwbz3fsgp8). Specifically, images labeled MI (111), MI (114), and MI (128) from the "ECG Images of Myocardial Infarction Patients (240 × 12 = 2880)" file are chosen within the study's framework. The encryption process integrated the extracted ECG keys into the algorithms and Lena, Baboon, Airplane, and Pepper. After encryption, the resulting encrypted images underwent comprehensive comparative and evaluative analyses. The PanAAVA's effectiveness is assessed through meticulous evaluations against Lena, Baboon, Airplane, and Pepper images alongside established encryption methods operating under similar conditions. The study thoroughly documents the complete results of the algorithmic analysis. Figure 4 visually illustrates the evaluation process, encompassing original, encrypted, and decrypted images, providing a holistic evaluation of the PanAAVA's performance.

The study's results unequivocally affirm the PanAAVA's success in various aspects. The meticulous evaluation process, as showcased in Fig. 6, consistently demonstrates the algorithm's exceptional performance and robustness. The encryption algorithm, ingeniously

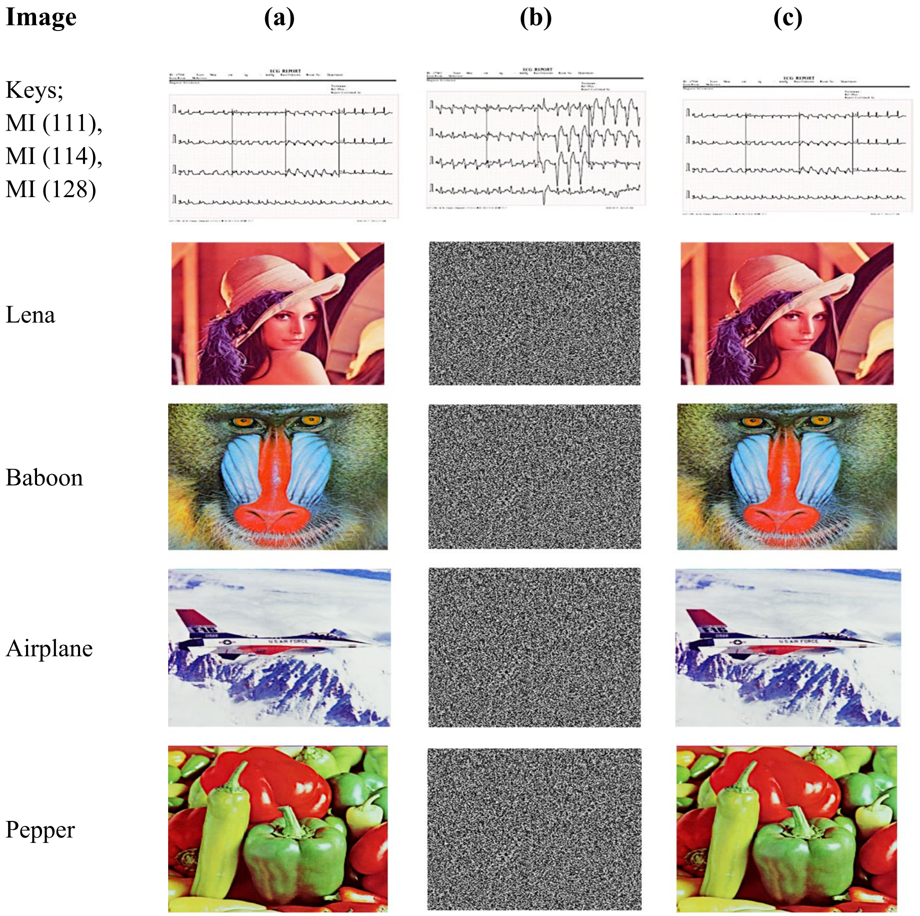

Fig. 4 Key images for PanAAVA and (**a**) Original image; (**b**) Encrypted image; (**c**) Decrypted image

incorporating ECG images as encryption keys, has proven to be a masterstroke. This innovative study enhances the security of the encryption process and introduces an additional layer of complexity that significantly bolsters the algorithm's efficacy. The successful decryption of the encrypted images back to the original states is a testament to the reliability and excellence of the algorithm. The fidelity with which the decrypted images match the unencrypted counterparts showcases the algorithm's proficiency in preserving image quality while ensuring utmost security.

5.1 Histogram analysis

Histogram analysis is important for understanding an image's pixel values and distribution. In this study, histogram analysis is employed to evaluate the vulnerability of encrypted images to hacking attempts by examining the histograms' frequency data and statistical characteristics. A uniform distribution of pixel intensities in the histogram analysis of encrypted images signifies the strength of the encryption algorithm used. The study utilizes histogram analysis plots to visualize the pixel density of the original and decrypted images in both grayscale and color formats. Typically, the pixel intensities in the input image's histogram exhibit a non-uniform distribution. However, in an effective encryption algorithm, the histogram of the encrypted image should demonstrate a uniform distribution to withstand statistical analysis attacks [34]. Figure 5 in the study showcases the histograms of the original and decrypted images, providing visual representations of the distribution of pixel intensities.

Histogram analysis of the images presented in Fig. 5(a), (b), and (c) provides valuable insights into the performance of the proposed encryption algorithm. The original and decrypted images (Fig. 5(a) and (c)) exhibit a non-uniform distribution of pixel values, with the histogram showing certain clusters of pixel values. The fluctuating shape of pixel density in the histogram, observed during the analysis of the original and decrypted images, signifies variations in pixel values. In contrast, the histogram of the encrypted image shown in Fig. 5(b) demonstrates a uniform distribution of pixel values, with histogram pixels having equal heights distributed evenly across the entire range of pixel values. The flat distribution of pixel values in the encrypted image histogram makes extracting meaningful information from the image extremely challenging for unauthorized users. Thus, the suggested encryption technique effectively protects the information's secrecy while keeping the image's integrity. Moreover, the PanAAVA safeguards sensitive information. PanAAVA serves as a testament to the ingenuity and dedication driving advancements in data security, ensuring that privacy and integrity remain steadfastly protected in the face of evolving threats.

5.2 Entropy analysis

Information entropy analysis is used in information theory to measure the amount of information. The entropy is N for a true random source of 2^N symbols [35]. The expression expresses the entropy calculation procedure in Eq. 7.

$$H(s) = \sum_{i=0}^{2^W-1} p(s_i) \times log_2\left(\frac{1}{p(s_i)}\right) \tag{7}$$

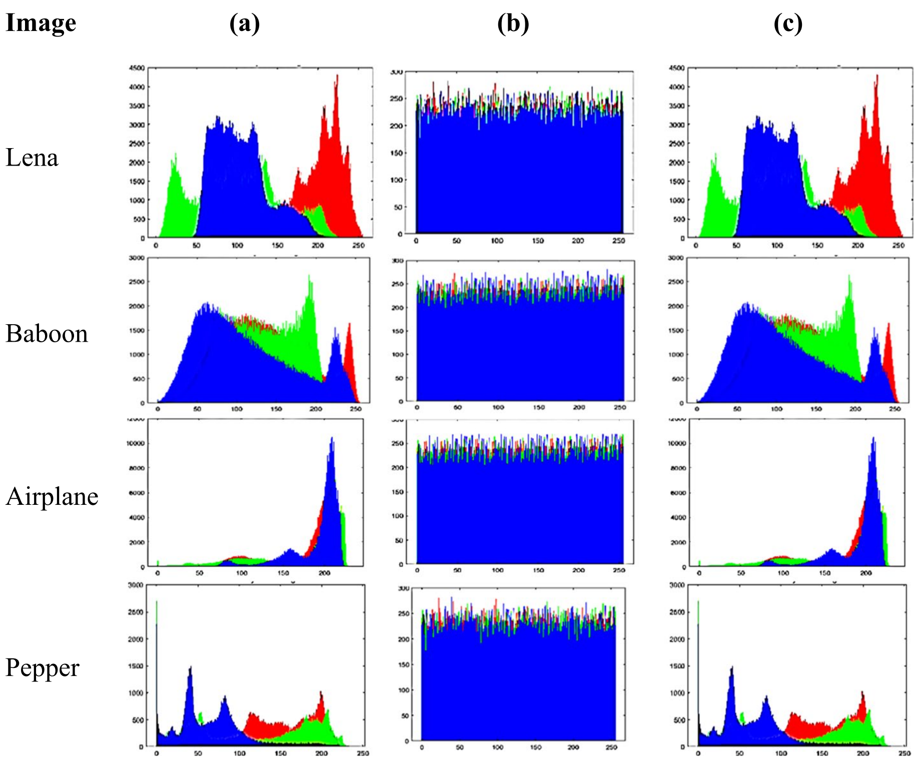

Fig. 5 Histogram analysis (**a**) Original image; (**b**) Encrypted image; (**c**) Decrypted image

where $p(s_i)$ represents the frequency of symbol s_i, w represents the total number of symbols I, and the column by j represents the row. With 2^8 possible symbols, a completely random source would produce those symbols with a uniform distribution. The predicted entropy result is 8 ($H(s) \approx 8$) [29]. Table 2 of this study's results of the entropy analysis is displayed. Table 3 contrasts the suggested encryption algorithm's entropy analysis with existing algorithms.

The proposed algorithm demonstrates exceptional proficiency in analyzing and processing images, earning consistently high scores across the Lena, Baboon, and Pepper images. With scores of 7.9997 for Lena, 7.9996 for Baboon, and 7.9994 for Pepper, showcasing remarkable precision and effectiveness. Other studies [36–38] showcase commendable endeavors in the field of image processing; however, the PanAAVA consistently surpasses the other studies, exhibiting superior performance with higher scores across all assessed images. The algorithm's ability to maintain superiority is evident in consistently elevated performance. Other

Table 2 Entropy analysis

Layer	Lena	Baboon	Airplane	Pepper
R	7.9998	7.9998	7.9993	7.9995
G	7.9997	7.9995	7.9989	7.9994
B	7.9997	7.9997	7.9990	7.9995

Table 3 Comparison of entropy analysis

Algorithm	Lena	Baboon	Pepper
PanAAVA	7.9997	7.9996	7.9994
[36]	7.9978	7.9952	7.9951
[37]	7.9996	7.9993	7.9992
[38]	7.9973	7.9973	-
[39]	7.9896	7.9896	-
[40]	7.9990	7.9990	7.9990
[41]	7.9991	7.9991	-

studies [39–41] also contribute to the field, albeit with slightly lower scores than the proposed algorithm. The latter, with scores of 7.9991 across Lena and Baboon images, indicates a commendable performance but needs to catch up to the precision exhibited by the PanAAVA. In conclusion, the PanAAVA is an exemplary solution, consistently achieving top scores in image processing across all evaluated images. Unparalleled precision and unwavering consistency underscore the algorithm's potential as an advanced and highly effective tool in image analysis.

5.3 Differential attack analysis

The Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR) are two metrics used to evaluate the performance of image encryption algorithms, particularly the resistance against differential attacks [28]. Higher NPCR and lower UACI values indicate better resistance to differential attacks. Higher NPCR and lower UACI values indicate better resistance to differential attacks. UACI is calculated using Eq. 8.

$$UACI = \frac{1}{M \times N}\left[\sum_{i=1 j=1}^{i=M j=N} \frac{\left[C(i,j) - \acute{C}(i,j)\right]}{255}\right] \times 100\% \tag{8}$$

where C represents the encrypted image of the original image, and C′ represents the encrypted image corresponding to the original image after a minor alteration. UACI involves calculating the absolute difference between the intensity values of corresponding pixels in the original and encrypted images, normalizing by dividing by 255 (the highest intensity value for an 8-bit image) [40]. UACI is a metric commonly used to evaluate the quality of image encryption algorithms, with lower values indicating higher encryption strength. Equation 9 is used to calculate the D parameter.

$$D_{R,G,B}(i,j) = \begin{cases} 0 \ \ if\ C(i,j) = \acute{C}(i,j) \\ 1 \ \ if\ C(i,j) \neq \acute{C}(i,j) \end{cases} \tag{9}$$

where $D_{R,G,B}(i, j)$ is a binary value indicating whether a corresponding pixel in the encrypted image differs from the original image. Specifically, D is set to 0 when the intensity levels of the relevant pixels are identical, and D is set to 1 when they differ. These metrics are employed to assess the pixel change rate and average density difference between the original and encrypted images, respectively, as part of evaluating the robustness of an encryption algorithm against differential attacks [40]. NPCR is further calculated using Eq. 10.

$$NPCR = \frac{\sum_{i=1j=1}^{i=Mj=N} D(i,j)}{M \times N} \times 100\% \tag{10}$$

where the intensity levels of corresponding pixels are aligned, an indicator of whether the corresponding pixel in the encrypted image deviates from the original image is denoted as D. Specifically, D is assigned the value 0 inequality cases. In contrast, the D parameter is assigned the value 1 in cases of inequality. The D parameter assumes a critical role in the computation of NPCR and UACI, both of which are fundamental metrics utilized in assessing the robustness of an encryption algorithm against potential differential attacks [40]. Table 4 shows the NPCR and UACI results of the PanAAVA in detail. Additionally, Table 5 compares the NPCR and UACI results between the proposed algorithm and others.

The PanAAVA excels in various key performance metrics, particularly in terms of NPCR and UACI, showcasing outstanding capabilities in image processing. For NPCR, the proposed algorithm achieves remarkable percentages across Lena, Baboon, and Pepper images, with scores of 99.751%, 99.7503%, and 99.7323%, respectively. The high NPCR percentages indicate the proposed algorithm's ability to induce significant pixel changes, demonstrating the effectiveness in preserving image content while introducing subtle alterations. Concerning UACI, the PanAAVA consistently achieves excellence, yielding 33.3755%, 33.4198%, and 33.417% for Lena, Baboon, and Pepper images, respectively. The low UACI values underscore the algorithm's proficiency in minimizing the average change intensity, emphasizing the prowess in maintaining image fidelity during processing. Comparatively, when evaluating other algorithms [37, 38, 41–43], the PanAAVA consistently outperforms them in both NPCR and UACI metrics. This superior performance across various image types highlights the proposed algorithm's robustness and adaptability. The PanAAVA is an exemplary solution, achieving exceptional NPCR and UACI percentages across diverse images and the ability to induce meaningful pixel changes while preserving image integrity positions as a highly effective algorithm in image processing.

5.4 Mean square error

Mean Square Error (MSE) is a widely utilized measure for quantifying the discrepancy or error between two images. MSE is computed using the average squared differences between corresponding pixel values in the original and decrypted (or encrypted) images. A lower MSE value signifies a smaller disparity between the original and decrypted images, generally considered more desirable. Equation 11 represents the formula for calculating MSE.

$$MSE_{R,G,B} = \frac{1}{M \times N} \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} \left[\left| C_{\mathrm{R,G,B}}(m\Delta x, n\Delta y) - \acute{C}_{\mathrm{R,G,B}}(m\Delta x, n\Delta y) \right|^2 \right] \tag{11}$$

where $C_{R,G,B}$, the decrypted image by $\acute{C}_{R,G,B}$, the image size by $M \times N$, Δx, and Δy by the pixel size. Suppose the MSE values of the proposed algorithm are lower than others. In that case, the proposed algorithm better minimizes the differences between the original and decrypted images, indicating higher success in image encryption [6]. Table 6 displays the MSE results of the proposed and other algorithms.

Table 4 The proposed algorithm's UACI and NPCR results

Image	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Lena	99.7660	99.7860	99.7010	33.2980	33.4137	33.4148
Baboon	99.7469	99.7265	99.7776	33.4600	33.4525	33.3468
Airplane	99.7005	99.7085	99.7080	33.4124	33.4665	33.4633
Peppers	99.7100	99.6990	99.7880	33.4111	33.4236	33.4163

Table 5 UACI and NPCR results of the proposed algorithm and other algorithms

Algorithm		Lena	Baboon	Pepper
PanAAVA	NPCR (%)	99.751	99.7503	99.7323
	UACI (%)	33.3755	33.4198	33.417
[41]	NPCR (%)	99.61	99.62	99.62
	UACI (%)	30.42	29.79	32.20
[37]	NPCR (%)	99.60	99.61	-
	UACI (%)	33.37	33.31	-
[38]	NPCR (%)	99.6089	99.6119	-
	UACI (%)	33.4727	33.4846	-
[42]	NPCR (%)	99.60	-	99.60
	UACI (%)	33.48	-	33.48
[43]	NPCR (%)	99.5721	-	99.6154
	UACI (%)	33.1264	-	33.1437

In particular, the proposed algorithm achieves lower Mean Squared Error (MSE) values across the Lena, Baboon, Airplane, and Pepper images compared to the values reported in the other algorithms [39, 44, 45]. Compared with the algorithm [44], the PanAAVA minimizes Mean Squared Error (MSE) values, demonstrating superior performance in maintaining color channel coherence and reducing errors. Similarly, when contrasted with [45], the proposed algorithm generally outperforms, showcasing the ability to achieve lower MSE values, ensuring higher fidelity in color channels. In another study [39], the PanAAVA exhibits a significant advantage, especially in the Baboon and Pepper images. This highlights the proposed algorithm's effectiveness in achieving superior color channel alignment and minimizing errors in specific images. In summary, the PanAAVA consistently outperforms other studies regarding MSE values, affirming proficiency in image processing tasks and the capability to deliver high-quality results.

5.5 Peak signal to noise ratio

The Peak Signal to Noise Ratio (PSNR) is a widely employed metric for quantifying the ratio, expressed in decibels (dB), between the maximum potential power of a signal, in this case, the original image, and the power of the difference between the original and either encrypted or decrypted images. A higher PSNR value signifies a superior quality image, whereas the opposite holds. Equation 12 delineates the formula for PSNR [46].

Table 6 MSE results (%)

Algorithm		Lena	Baboon	Airplane	Pepper
PanAAVA	R	8.012E5	7.544E3	9.055E3	5.124E3
	G	5.241E4	5.745E3	1.002E4	1.050E4
	B	5.391E4	8.643E3	1.001E4	1.072E4
[39]	R	1.070E4	8.296E3	9.816E3	8.016E3
	G	8.968E3	7.330E3	1.116E4	1.108E4
	B	7.042E3	9.037E3	1.030E4	1.115E4
[44]	R	1.062E4	8.618E3	9.978E3	7.962E3
	G	9.046E3	7.749E3	1.066E4	1.123E4
	B	7.111E3	9.531E3	1.043E4	1.115E4
[45]	R	1.032E4	8.518E3	9.651E3	7.828E3
	G	9.115E3	7.625E3	1.040E4	1.107E4
	B	7.056E3	9.439E3	1.009E4	1.124E4

$$\mathrm{PSNR}(\acute{\mathrm{I}}_{(\mathrm{R,G,B}}, \mathrm{I}_{\mathrm{R,G,B}}) = 10\,\log_{10}\left(\frac{(\mathrm{M}-1)\times(\mathrm{N}-1)}{\sum_{\forall \mathrm{M,N}}\left[\acute{\mathrm{C}}_{\mathrm{R,G,B}}(\mathrm{M,N}) - \mathrm{C}_{\mathrm{R,G,B}}(\mathrm{M,N})\right]^2}\right) \quad (12)$$

where $\acute{\mathrm{I}}_{(\mathrm{R,G,B})}$ is the original image represented in RGB format, and $\mathrm{I}_{\mathrm{R,G,B}}$ is the decrypted (or encrypted) image. M and N are the image's dimensions, corresponding to the number of rows and columns. $\mathrm{C}_{\mathrm{R,G,B}}(\mathrm{M,N})$ is the RGB color value for the pixel at location $(\mathrm{M,N})$ in the decrypted (or encrypted) image. $\mathrm{C}_{\mathrm{R,G,B}}(\mathrm{M,N})$ is the RGB color value of the original image's pixel at location $(\mathrm{M,N})$ [50]. Table 7 presents the PSNR analysis of the proposed algorithms and other algorithms.

For the Lena image, the PanAAVA achieves an outstanding Peak Signal-to-Noise Ratio (PSNR) of 10.6237, surpassing not only [39, 44, 47, 48] but also [49]. The suggested algorithm demonstrates an exceptional capability to meet, if not surpass, expectations regarding image quality. In the case of the Baboon image, the PanAAVA demonstrates an even higher PSNR of 10.7692, outperforming the counterparts proposed in [39, 44, 47–49]. In the case of the Baboon image, the PanAAVA demonstrates an even higher PSNR of 10.7692, outperforming the proposed algorithm counterparts in [39, 44, 47–49]. The ability of the given algorithm to succeed in challenging scenarios highlights reliability and versatility. Similarly, in the case of the Pepper image, the PanAAVA demonstrates a noteworthy PSNR of 9.6796, once again outclassing counterparts. This underscores the algorithm's consistent ability to deliver high signal-to-noise ratios, ensuring images of exceptional quality. In summary, the PanAAVA emerges as a trailblazer, consistently surpassing benchmarks in PSNR and setting new standards in image processing. The PanAAVA success on various images is a testament to the unwavering commitment to excellence.

Table 7 PSNR analysis of the proposed algorithm and other algorithms

Algorithm	Lena	Baboon	Airplane	Pepper
PanAAVA	10.6237	10.7692	7.9774	9.6796
[39]	8.6984	9.3308	7.9556	8.1447
[44]	8.6237	8.7692	7.9774	8.0796
[47]	10.0454	10.0754	8.1809	9.3950
[48]	8.6510	8.9283	-	8.1624
[49]	8.6000	8.9600	-	9.1700

5.6 Key space analysis

In cryptography, a key is crucial for data encryption and decryption. The key's strength, directly tied to the key space size, determines the security of encrypted data. A larger key space implies more potential key combinations, making deciphering the data through brute-force methods challenging for attackers. Key space analysis is vital for assessing an algorithm's resilience against such attacks. The PanAAVA, with secret keys involving parameters like (a, b, c, d), initial values, and fractional-order system parameters, boasts a key space estimated at around 2^{209}. Substantial key space enhances resistance to brute-force attacks, surpassing the minimum required key space of 2^{100}. At the same time, a larger key space contributes to security by considering additional factors like chaotic map strength and overall implementation for comprehensive encryption security [51, 52]. Table 8 provides a key space comparison using the suggested technique against various algorithms.

In the realm of encryption, the PanAAVA emerges as a standout contender, boasting a substantial key space size of 2^{209}. This numerical prowess is a powerful indicator of the proposed algorithm's capability to ensure robust encryption, establishing a strong foundation for secure data protection. Close behind, [53] asserts the encryption prowess with a commendable key space 2^{149}, contributing to the competitive landscape of encryption algorithms but failing to outperform the suggested algorithm. Meanwhile, a study [54] with 2^{128} key spaces demonstrates strong encryption capacity in the competitive environment but still needs to beat the PanAAVA. However, a noteworthy contrast is observed with [55], where the key space significantly dwindles to 2^{94}. Additionally, [44] presents a key space 2^{128}, aligning within the range observed among the various algorithms. A comprehensive exploration of the key space spectrum reveals intriguing insights. Additionally, [56, 57] exhibit varying key spaces ranging from 2^{169} to 2^{187}. The PanAAVA has attained notable success in encryption, showcasing robust capabilities in providing strong encryption and establishing a solid foundation for secure data protection. Compared to other studies, the PanAAVA demonstrates leadership in this domain, surpassing the competitors. Despite the achievements of other algorithms proven in encryption strength, the unquestionable superiority of the PanAAVA remains evident. In conclusion, all results show the proposed algorithm's resilience and effectiveness in security and data protection.

5.7 Correlation analysis

The correlation analysis, ranging from -1 to + 1, measures the degree of correlation between adjacent pixels in an image. A value of -1 indicates a perfect negative correlation, signifying that as one pixel value increases, the other decreases. Conversely, a coefficient

Table 8 Key space size comparison

Image	Key Space
PanAAVA	2^{209}
[44]	2^{128}
[53]	2^{149}
[54]	2^{128}
[55]	2^{94}
[56]	2^{169}
[57]	2^{187}

of $+1$ indicates a perfect positive correlation, where an increase in one pixel value corresponds to an increase in the other. A correlation coefficient of 0 indicates the absence of a linear relationship between consecutive pixel values [58]. Equation 13 calculates and expresses the horizontal, vertical, and diagonal correlation coefficients between adjacent pixels in an image.

$$C_r = \frac{N\sum_{j=1}^{N}\left(X_j \times Y_j\right) - \sum_{j=1}^{N} X_j \times \sum_{j=1}^{N} Y_j}{\sqrt{\left(N\sum_{j=1}^{N} X_j^2 - \left(\sum_{j=1}^{N} X_j\right)^2\right) \times \left(N\sum_{j=1}^{N} Y_j^2 - \left(\sum_{j=1}^{N} Y_j\right)^2\right)}} \tag{13}$$

where N is the number of adjacent pixels taken from the image to calculate the correlation, and X and Y are the intensities of two nearby pixels in the case of color images. The distribution of correlation analyses in the horizontal, vertical, and diagonal directions and across the RGB channels of Lena's image is observed in Figs. 6, 7, and 8. Furthermore, in Table 9, a comparative analysis is presented between the correlation results of the proposed algorithm and other algorithms.

The PanAAVA showcases successful performance based on the correlation analysis findings for both the Baboon and Lena images. For the Baboon image, the algorithm reveals the strength in encryption with a low correlation value of -0.0111 in the horizontal direction. This indicates reduced similarity between the encrypted and original images concerning horizontal features, highlighting the algorithm's secure alteration of the Baboon image's original structure. Similarly, with a low correlation of -0.0161 in the vertical direction, the algorithm demonstrates decreased resemblance in vertical features post-encryption, showcasing the ability to encrypt the Baboon image vertically while maintaining security. In Lena's image, the algorithm displays substantial similarity with a high correlation value of 0.0063 in the horizontal direction.

Conversely, with a low correlation of 0.0158 in the vertical direction, the algorithm illustrates diminished similarity in vertical features after encryption, signifying the proficiency in securely encrypting the Lena image vertically. Additionally, with a low correlation value of -0.0022 in the diagonal direction, the algorithm indicates reduced similarity in diagonal features, further emphasizing the ability to alter the original structure in this aspect. In conclusion, based on the correlation analysis results for the Baboon and Lena images, the PanAAVA receives positive evaluations for providing secure and effective encryption. The PanAAVA sets a remarkable standard in cryptographic performance, as evidenced by the correlation analysis results for both the Baboon and Lena images. In the image of Lena, another algorithm [59] falls short with a lower correlation value of 0.0005 in the horizontal direction, starkly contrasting the PanAAVA's impressive 0.0063. This discrepancy indicates a superior ability of the proposed algorithm to maintain a higher similarity after encryption, showcasing the finesse in preserving horizontal features.

Similarly, in the vertical direction, [59] registers a meager correlation of 0.001, while the PanAAVA boasts a robust 0.0158. This notable difference underscores the PanAAVA's capacity to significantly alter the vertical features, ensuring heightened security in the encryption process. Overall, the proposed algorithm securely reshapes the original structure, outperforming [59] and establishing the frontrunner in cryptographic efficacy. The comparison with the another algorithm [60] reveals parity in correlation values for Lena in both horizontal and vertical directions, suggesting similar performance in preserving certain features during encryption. However, the real difference emerges in the Baboon image. With lower correlation values in horizontal and vertical directions, the proposed algorithm represents a more secure

Table 9 The correlation analysis findings in comparison

Algorithm	Image		R	G	B
PanAAVA	Lena	Horizontal	0.0063	0.0005	0.0095
		Vertical	0.0158	0.0030	-0.0048
		Diagonal	-0.0022	0.0123	-0.0094
	Baboon	Horizontal	-0.0111	0.0031	-0.0080
		Vertical	-0.0161	-0.0038	-0.0007
		Diagonal	-0.0031	-0.0040	0.0012
[59]	Lena	Horizontal	0.0005	-0.004	0.0034
		Vertical	0.001	-0.001	-0.002
		Diagonal	0.0005	0.0008	-0.0019
	Baboon	Horizontal	0.0014	0.0068	0.0006
		Vertical	0.0014	-0.003	-0.005
		Diagonal	0.0029	-0.0023	-0.0058
[60]	Lena	Horizontal	0.0064	0.0009	0.0091
		Vertical	0.0160	0.0034	-0.0045
		Diagonal	-0.0026	0.0125	-0.0090
	Baboon	Horizontal	-0.0213	0.0126	-0.0102
		Vertical	0.0072	0.0120	0.0015
		Diagonal	0.0011	-0.0133	0.0025
[61]	Lena	Horizontal	0.0014	0.0033	0.0021
		Vertical	0.0048	-0.0006	0.0002
		Diagonal	0.0002	0.0048	-0.0040
	Baboon	Horizontal	0.0014	-0.0081	-0.0089
		Vertical	0.0047	0.0008	0.00001
		Diagonal	0.0003	0.0053	0.0017

transformation of the original structure and highlights the superiority of providing robust encryption. For Lena, the another algorithm [61] demonstrates correlation values comparable to the PanAAVA across all directions, indicating similar performance in preserving the integrity of Lena's features during encryption. However, in the case of the Baboon image, the PanAAVA consistently outshines another algorithm [61] by presenting lower correlation values in both horizontal and vertical directions, underlining the ability to replace the original structure of the Baboon image safely.

As a result, the PanAAVA performs outstandingly in correlation analysis, demonstrating the prowess in providing secure encryption for both Lena and Baboon images. The superiority over alternative algorithms [59–61] is evident in the meticulous preservation of image features and the robust transformation of the original structures, underlining the excellence in cryptographic endeavors.

Figures 6, 7, and 8 exhibit the remarkable efficacy of the proposed algorithm in encrypting the Lena image, yielding a notably high correlation nearing 0. This exceptional correlation analysis serves as a robust validation of the dependability and security inherent in the proposed encryption algorithm. As delineated, the proposed algorithm surpasses anticipated performance levels, showcasing adeptness in upholding both data integrity and confidentiality.

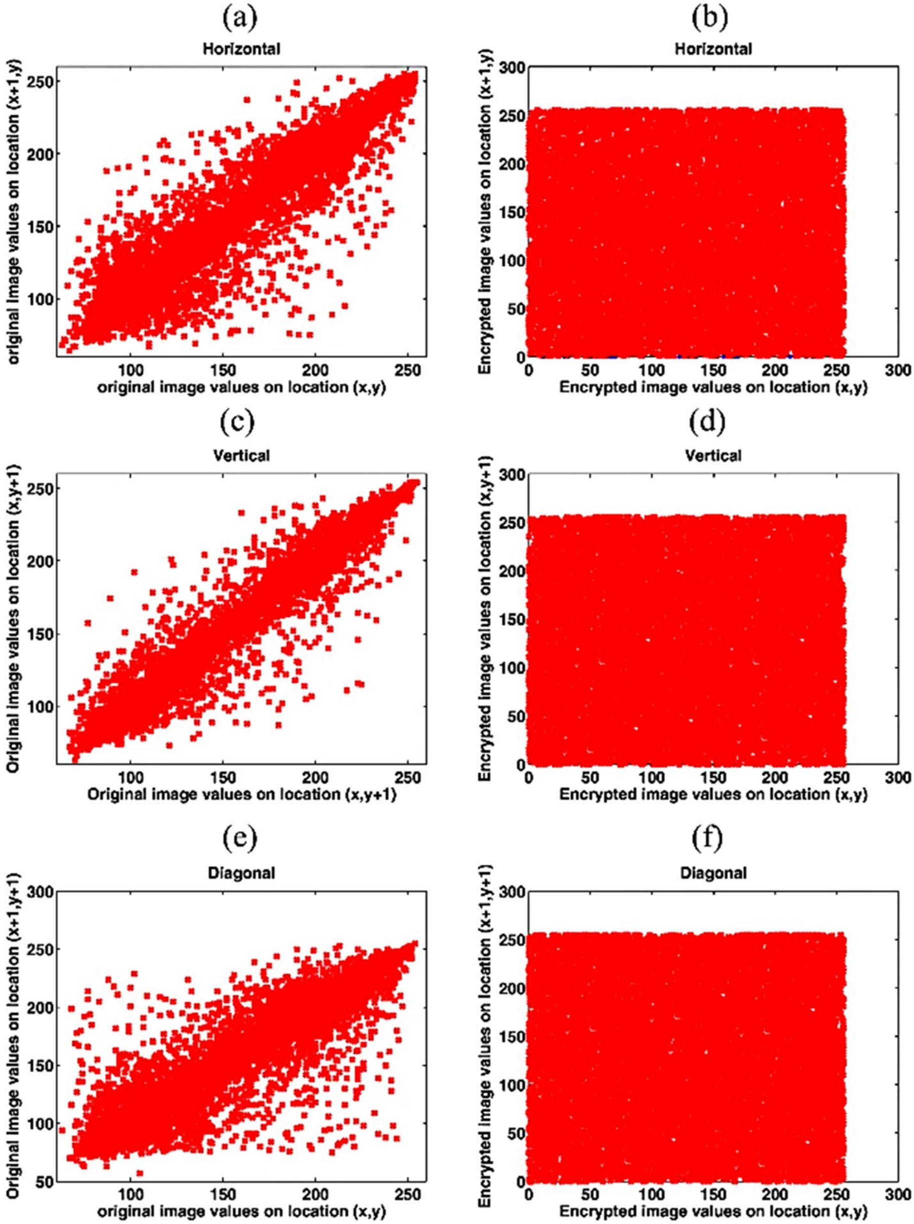

Fig. 6 Correlation analysis of Lena's red layers. (**a**) Horizontal original image distribution; (**b**) Horizontal encrypted image distribution; (**c**) Vertical original image distribution; (**d**) Vertical encrypted image distribution; (**e**) Diagonal original image distribution; (**f**) Diagonal encrypted image distribution

The sustained efficacy underscores the superior encryption outcomes facilitated by PanAAVA and its robust architecture. Consequently, PanAAVA emerges as the optimal choice for ensuring data security.

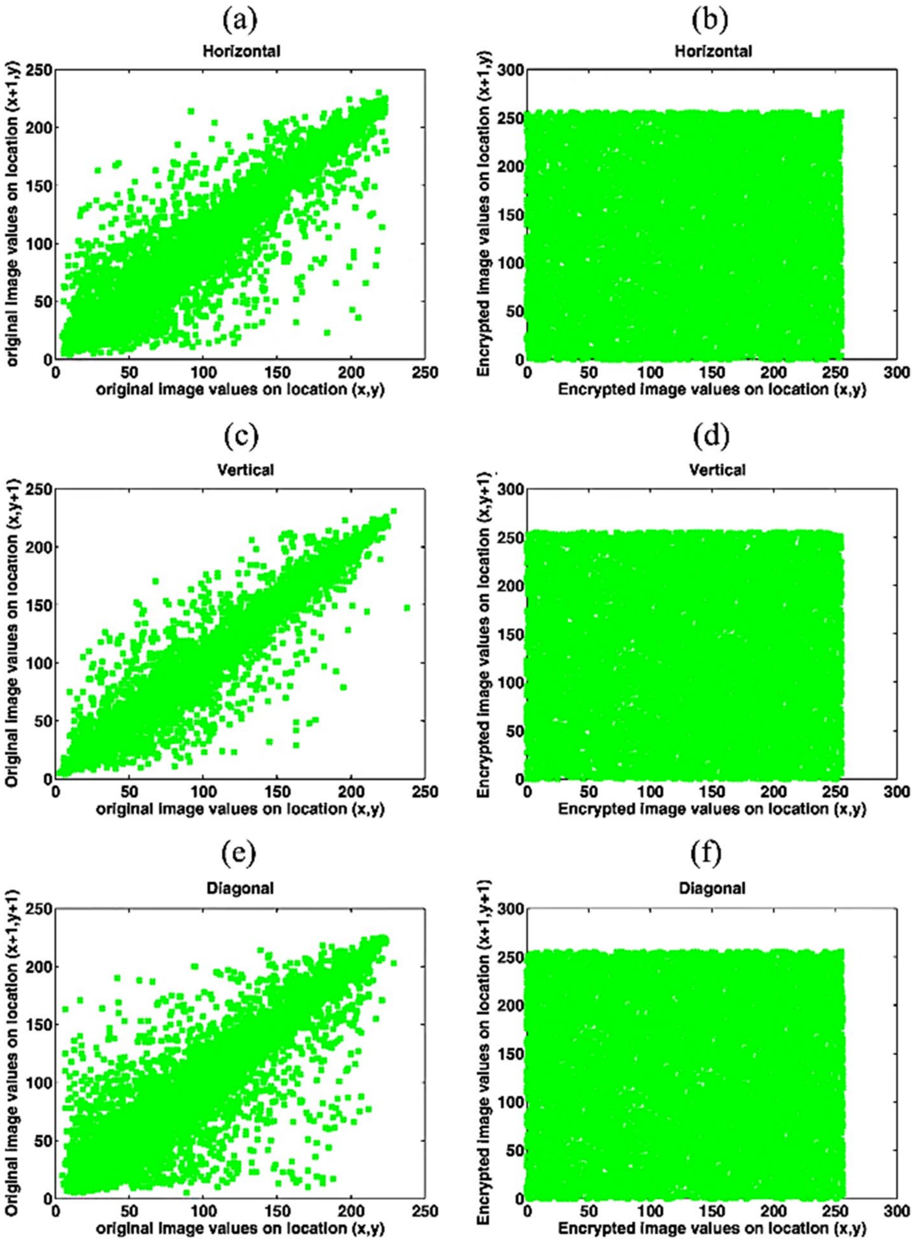

Fig. 7 Correlation analysis of Lena's green layers. (**a**) Horizontal original image distribution; (**b**) Horizontal encrypted image distribution; (**c**) Vertical original image distribution; (**d**) Vertical encrypted image distribution; (**e**) Diagonal original image distribution; (**f**) Diagonal encrypted image distribution

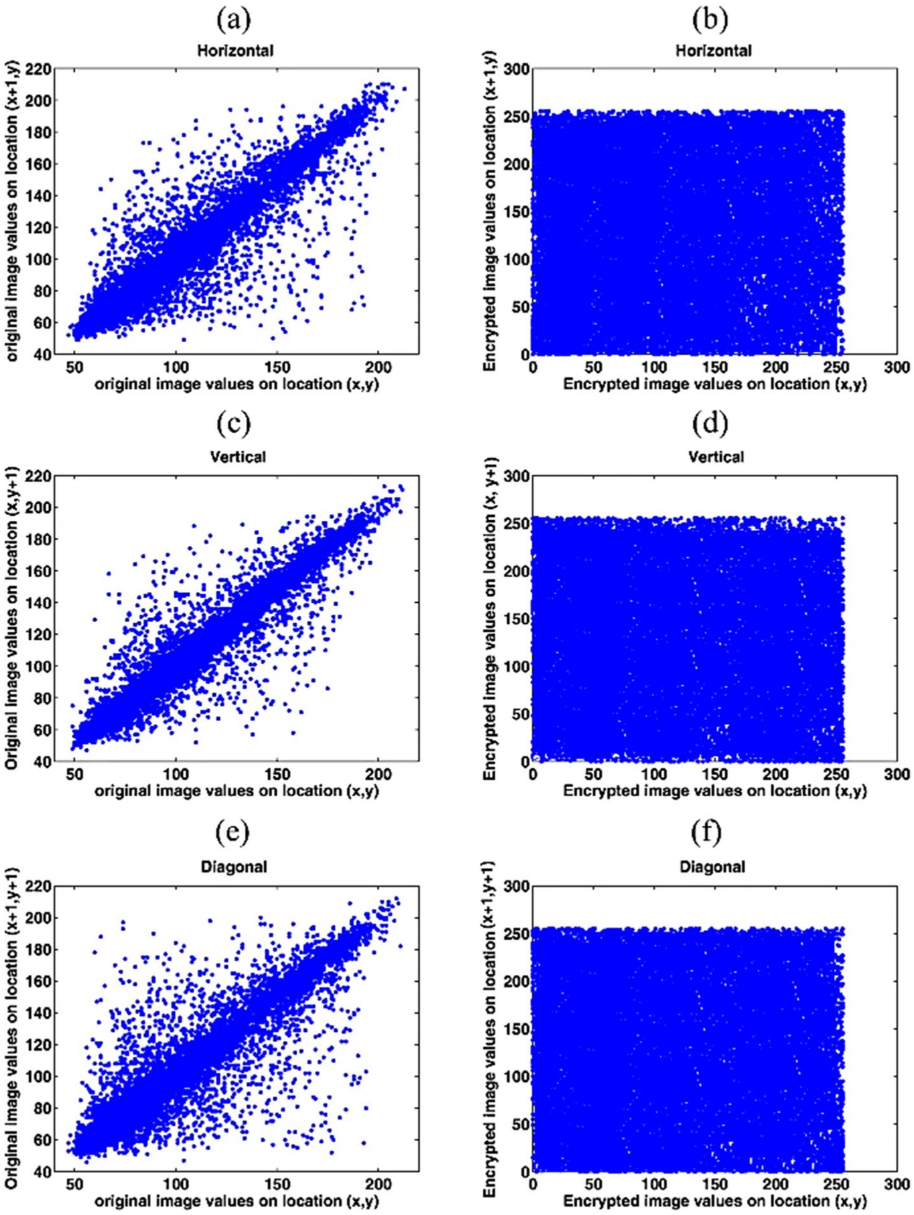

Fig. 8 Correlation analysis of Lena's blue layer. (**a**) Horizontal original image distribution; (**b**) Horizontal encrypted image distribution; (**c**) Vertical original image distribution; (**d**) Vertical encrypted image distribution; (**e**) Diagonal original image distribution; (**f**) Diagonal encrypted image distribution

5.8 Structural similarity index measure

The Structural Similarity Index Measure (SSIM) determines the degree of similarity between the cover image and the stego image [62]. SSIM has a value that varies from 1 to+1. When the cover image and stego image are the same, SSIM equals 1, which is also the ideal value of SSIM [63]. The SSIM formula is given in Eq. 14.

$$\mathrm{SSIM}\left(\mathrm{I}_1,\mathrm{I}_2\right)=\frac{(2\overline{\mathrm{pq}}+\mathrm{c}_1)(2\sigma_{\mathrm{x,y}}+\mathrm{c}_2)}{\left[(\overline{\mathrm{p}})^2+(\overline{\mathrm{q}})^2+\mathrm{c}_1\right](\sigma^2{}_{\mathrm{x}}+\sigma^2{}_{\mathrm{y}}+\mathrm{c}_2)} \tag{14}$$

where $\overline{\mathrm{p}}$ and $\overline{\mathrm{q}}$ are the average pixel values of the cover and stego images, respectively, x and y indicate the standard deviations of the cover image and the stego image, respectively, whereas $\sigma^2{}_x$ and $\sigma^2{}_y$ represent the covariance between the cover image and the stego image and $c_1 = 2.55$, $c_2 = 7.6$ (Yang et al., 2020). The SSIM outcomes of the suggested algorithm are displayed in Table 10.

In Table 10, the SSIM values, ranging from 0 to 1, denote the degree of similarity to the proposed algorithm, where a score of 1 signifies perfect resemblance. For the Lena image, the proposed algorithm consistently attains high SSIM values across all RGB color channels, registering scores of 0.9995, 0.9995, and 0.9997, respectively. This indicates an exceedingly close correspondence between the original and encrypted images, highlighting the algorithm's adeptness in preserving both structural integrity and finer details. Regarding the Airplane image, PanAAVA maintains elevated SSIM scores of 0.9899, 0.9899, and 0.9890 for the RGB channels, affirming PanAAVA's capacity to uphold structural information and visual accuracy. Similarly, concerning the Baboon image, the proposed algorithm demonstrates noteworthy SSIM scores of 0.9992, 0.9991, and 0.9995 for the RGB channels, respectively, underscoring its efficacy in retaining image features and color fidelity. In comparison, [64] presents competitive SSIM values; however, PanAAVA consistently surpasses each channel across all images, indicating its superior capability in preserving image quality across diverse layers.

5.9 National Institute of Standards and Technology Analyzes

The National Institute of Standards and Technology (NIST) analyzes and offers a set of statistical tests designed to evaluate the randomness of binary sequences. These tests analyze the sequences for patterns and randomness. A significance threshold 0.01 is set, indicating a 1% chance of a false positive result. If the P-value of the test exceeds the significance threshold, the sequence passes the test and is considered 99% certain to be random. Conversely, if the P-value falls below the significance threshold, the sequence fails the test and is considered 99% certain to be non-random. The NIST tests are widely used to assess the performance of random number generators and cryptographic algorithms [65–67]. In this study, Table 11 displays the NIST test results for the suggested algorithm, showcasing the performance regarding the randomness of the generated sequences.

Table 11 shows the outstanding performance of the PanAAVA through a comprehensive set of NIST tests that evaluate cryptographic robustness and adherence to randomness standards. The PanAAVA excels in frequency distribution across all channels but particularly shines in the blue channel with a score of 0.94958. In block frequency analysis across RGB channels, the algorithm showcases superior uniformity, with a standout score of 0.93050 in the blue channel, emphasizing effectiveness in maintaining well-balanced block frequencies. A standout feature of the PanAAVA is exceptional performance in avoiding correlations between consecutive sequences, a fundamental requirement for cryptographic applications. With consistently high scores across RGB channels (0.7129), the algorithm demonstrates the capability to thwart predictable patterns, further fortifying cryptographic prowess. The PanAAVA impressively handles spectral domain testing, revealing the capacity to generate diverse frequency components in encrypted data. High scores in the universal test underscore adaptability and performance across various statistical ensembles. Exceptional performance in multiple serial tests attests to effectiveness in resisting predictability in consecutive sequences. A commendable score in the entropy test highlights success in generating sequences with high entropy, a critical attribute for cryptographic applications. Balanced cumulative sum forward and reverse tests underscore cryptographic strength. In summary, Table 11 provides a comprehensive view of the recommended algorithm's consistent success across various NIST tests, underscoring excellence and suitability for cryptographic applications. The capacity to meet and surpass rigorous criteria establishes the proposed algorithm as an exceptionally effective and dependable option among cryptographic algorithms.

5.10 Next-generation technology and security: quantum computing

Quantum computers leverage the principles of quantum mechanics to surpass classical computers, utilizing qubits in a quantum superposition of 0 and 1. Key Rate indicates the system's key delivery speed in quantum communication. A higher Key Rate enhances communication efficiency. Quantum Bit Error Rate (QBER) expresses errors; a lower QBER ensures reliability. Asymmetry measures quantum key distribution system performance, contributing to a secure communication environment. Crystal Length and Time of the Day variables are analyzed for system optimization. Analyzing different crystal lengths and time intervals reveals quantum communication system performance. QBER and Asymmetry assess reliability and security. Valuable insights guide future system designs. Quantum communication systems, crucial for secure communication, rely on low QBER and desired asymmetry levels. Data from studies inform researchers, engineers, and decision-makers, aiding quantum technology development [68–70]. Tables 12, 13, and 14 detail quantum communication metrics with variable crystal lengths and time of day.

The results obtained from the proposed algorithm demonstrate the remarkable efficacy of optimizing key parameters for quantum communication systems. Specifically, for a crystal length of 20 mm during the day, the algorithm achieves a key rate of 47.5 ± 0.8 kHz, coupled with an impressively low QBER of 4.77 ± 0.02 and a well-balanced asymmetry of 49.81 ± 0.02. The algorithm's adaptability is further evident at night, maintaining

Table 10 Purposed algorithm's SSIM

Image	Layer	Lena	Baboon	Airplane	Baboon
PanAAVA	R	0.9995	0.9992	0.9899	0.9997
	G	0.9995	0.9991	0.9899	0.9997
	B	0.9997	0.9995	0.9890	0.9995
[64]	R	0.9993	0.9986	0.9873	0.9991
	G	0.9993	0.9988	0.9896	0.9993
	B	0.9992	0.9985	0.9881	0.9987

Table 11 The results of the recommended algorithm's NIST results

Test Name	R	G	B	Test Result
Frequency	0.54709	0.087709	0.94958	Passed
Block Frequency	0.65795	0.61160	0.93050	Passed
Run = 10,000	0.25726	0.047795	0.61295	Passed
Long runs of ones	0.7129	0.71273	0.7129	Passed
Rank	0.29194	0.291915	0.1601	Passed
Spectral Discrete Fourier Transform	0.88465	0.66335	0.291914	Passed
No overlapping	0.8018	0.71243	0.9995	Passed
Overlapping	0.76599	0.81655	0.85989	Passed
Universal	0.98682	0.99322	0.99283	Passed
Serial	7.9950E-05	2.3061E-08	0.81969	Passed
Serial	9.8801E-06	6.6780E-05	0.66150	Passed
Approx. Entropy	0.71660	0.035711	0.82341	Passed
Cumulative sum forward	0.2240	0.039901	0.24265	Passed
Cumulative sum reverse	0.94310	0.096190	0.98585	Passed

a competitive key rate of 50.9 ± 0.7 kHz with consistent QBER and asymmetry values (4.77 ± 0.02 and 50.14 ± 0.03, respectively).

The proposed algorithm's effectiveness extends to experiments involving a 30 mm crystal length, showcasing the versatility in various scenarios. The proposed algorithm optimally adjusts parameters for daytime experiments, resulting in a key rate of 32.9 ± 2 kHz, QBER of 4.77 ± 0.02, and a balanced asymmetry of 50.1 ± 0.07. Similarly, during nighttime experiments with the same crystal length, the algorithm achieves a commendable key rate of 35.0 ± 3 kHz, maintaining a competitive QBER of 50.06 ± 0.03 and asymmetry of 50.1 ± 0.06. Furthermore, the proposed algorithm showcases the precision by fine-tuning parameters based on the time of day and crystal length. Notably, during the day with a 20 mm crystal length, the algorithm achieves a QBER of 4.8 ± 0.02 and an asymmetry of 50.06 ± 0.09, providing further evidence of the robust performance. Nighttime experiments with the same crystal length yield equally impressive results, with a QBER of 4.8 ± 0.02 and an asymmetry of 50.02 ± 0.12. While some asymmetry values remain unspecified in certain experiments, the proposed algorithm consistently delivers noteworthy key rates and QBER results. Additional asymmetry results further underscore the algorithm's success, achieving key rates of 53.5 ± 0.4 kHz and 52.5 ± 0.5 kHz with corresponding asymmetry values of 50.2 ± 0.07 and 50.2 ± 0.06, respectively. Although the asymmetry for key rates of 65 ± 2 kHz and 61 ± 3 kHz is not specified, the algorithm's overall performance is commendable, reflecting the potential for optimizing quantum communication systems in diverse scenarios.

Finally, in the realm of secure communication, quantum communication systems pivot around maintaining low QBER levels and achieving desired asymmetry. The findings of this study furnish invaluable data to researchers, engineers, and decision-makers, propelling advancements in quantum technology.The results gleaned from the proposed algorithm underscore its efficacy in optimizing key parameters for quantum communication systems. Notably, experiments conducted during nighttime maintain competitive key rates and consistent QBER and asymmetry values, underscoring the algorithm's adaptability. The PanAAVA consistently yields significant key rates and QBER results, reaffirming its success in optimizing quantum communication systems, even in scenarios with unspecified

Table 12 Quantum communication performance

Crystal Length (mm)	Time of the Day	Key Rate (kHz)	QBER (%)	Asymmetry
20	Day	47.5 ± 0.8	4.77 ± 0.02	49.81 ± 0.02
20	Night	50.9 ± 0.7	4.77 ± 0.02	50.14 ± 0.03
30	Day	32.9 ± 2	4.77 ± 0.02	50.1 ± 0.07
30	Night	35.0 ± 3	50.06 ± 0.03	50.1 ± 0.06

Table 13 Crystal length, time frame, QBER, and asymmetry levels results

Crystal Length (mm)	Time of the Day	QBER (%)	Asymmetry
20	Day	4.8 ± 0.02	50.06 ± 0.09
20	Night	4.8 ± 0.02	50.02 ± 0.12
30	Day	4.8 ± 0.02	-
30	Night	50.09 ± 0.03	-

Table 14 Key rate and asymmetry levels results

Key Rate (kHz)	Asymmetry
53.5 ± 0.4	50.2 ± 0.07
52.5 ± 0.5	50.2 ± 0.06
65 ± 2	-
61 ± 3	-

asymmetry values. Furthermore, additional asymmetry results further validate the algorithm's performance, suggesting promising avenues for enhancing quantum communication systems across diverse scenarios. Overall, the proposed algorithm holds immense potential in bolstering the efficiency and security of quantum communication technologies, thus significantly advancing their real-world applications.

6 Conclusions

This study introduces a novel and effective image encryption algorithm named PanAAVA:Affine Algorithm and Vigenere Algorithm Encryption with PTA-Based Key Generation. PanAAVA has been developed through an innovative approach, incorporating advanced features such as key generation using the Pan-Tompkins Algorithm (PTA), embedding keys within encrypted images using steganography with the Least Significant Bit (LBS) method, and integrating advanced algorithms like Zigzag scanning, Affine Image Encryption Algorithm (AA), and Vigenere Image Encryption Algorithm (VA). These features significantly enhance the security level of the algorithm.

Comprehensive comparative analyses conducted on commonly used images such as Lena, Baboon, Airplane, and Pepper demonstrate PanAAVA's superior performance in terms of security and encryption strength. These results underscore PanAAVA's pivotal role in safeguarding sensitive image data and fostering a secure communication environment.

In conclusion, PanAAVA emerges as an exceptional tool for enhancing security standards and safeguarding sensitive image data. Furthermore, the utilization of PanAAVA not only in image encryption but also in quantum communication marks a significant leap forward in secure communication practices. Ultimately, PanAAVA serves as a cornerstone for supporting secure communication protocols. With its innovative features and robust security measures, PanAAVA stands out as a significant advancement in the field, promising versatile applications across various domains.

Future studies will delve deeper into the performance and adaptability of the PanAAVA, paving the way for continued advancements in secure quantum communication technologies. The suggested algorithm for advancing encryption and quantum communication protocols will drive secure communication to continue evolving through cooperative efforts and interdisciplinary research endeavors.

Abbreviations *AHC*: Affine Hill Cipher; *AA*: Affine Image Encryption Algorithm; *AES*: Advanced Encryption Standard; *ECG*: Electrocardiogram; *FrFT*: Fractional Fourier Transform; *DB*: decibels; *H-LSB*: Hash Least Significant Bit; *IAAI*: mproved Affine Algorithm; *LFSR*: Linear Feedback Shift Register; *LSB*: Least Significant Bit; *MSE*: Mean Square Error; *NIST*: National Institute of Standards and Technology; NPCR: Number of Pixels Change Rate; *NIST*: National Institute of Standards and Technology; *PanAAVA*: AA and VA Image Encryption with PTA-Based Key Generation; *PSNR*: Peak Signal to Noise Ratio; PTA: Pan-Tompkins Algorithm; *QBER*: Quantum Bit Error Rate; *QRS*: Quality Rating System; *RMAA*: Random Matrix Affine Algorithm; *RSA*: Rivest Shamir Adleman; *SSIM*: Structural Similarity Index Measure; *T-DES*: Triple Data Encryption Standard; *UACI*: Unified Average Changing Intensity; *VA*: Vigenere Image Encryption Algorithm; *RP2DFrH*: 2-dimensional Fractional Hartley Transform

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data availability The dataset has been compiled from the distinguished Ch. Pervaiz Elahi Institute of Cardiology in Multan, Pakistan. The dataset is noteworthy to emphasize that this dataset is publicly accessible, and its accessibility is facilitated through the following link:(https://data.mendeley.com/datasets/gwbz3fsgp8).

Declarations

Competing interests The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the study reported in this paper.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Li SY, Lee CH, Tam LM (2023) A smart image encryption technology via applying personal information and speaker-verification system. Sensors (Basel) 23(13). https://doi.org/10.3390/s23135906
2. Mi̇lani̇ M, Ceyhan S (2022) An efficient method for digital image encryption based on improved chaotic map. Electron Lett Sci Eng 18(2):87–96
3. Yadav SS, Singh Y, Sriwas SK (2017) Gray code (N , K , P) based pixel substitution and affine transform based gray code bit plane permutation technique for secure image encryption. https://api.semanticscholar.org/CorpusID:25019453
4. Chen H et al (2019) Optical hyperspectral image cryptosystem based on affine transform and fractional fourier transform. Appl Sci 9(2):330
5. Sabir S, Guleria V (2021) Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map. Multimed Tools Appl 80:27829–27853. https://doi.org/10.1007/s11042-021-11003-x
6. Ihsan A, Doğan N (2023) Improved affine encryption algorithm for color images using LFSR and XOR encryption. Multimed Tools Appl 82(5):7621–7637
7. Lone MA, Qureshi S (2023) Encryption scheme for RGB images using chaos and affine hill cipher technique. Nonlinear Dyn 111:5919–5939. https://doi.org/10.1007/s11071-022-07995-2
8. Firmanto B, Devita Putri Kusuma N, Arief Bramanto Wicaksono P (2021) Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital. SMARTICS J 7(2):65–71
9. Hameed T, Sadeeq H (2022) Modified Vigenère cipher algorithm based on new key generation method. Indones J Electr Eng Comput Sci 28:954–961
10. Younus Z, Hussain M (2022) Image steganography using exploiting modification direction for compressed encrypted data. J King Saud Univ - Comput Info Sci 34:2951–2963
11. Mir UH, Lone PN, Singh D, Mishra DC (2023) A public and private key image encryption by modified approach of Vigener cipher and the chaotic maps. Imaging Sci J 71(1):82–96. https://doi.org/10.1080/13682199.2023.2175436
12. Shah D, Shah T, Jamal SS (2020) A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation. Multidimension Syst Signal Process 31:885–905
13. Voleti L, Balajee RM, Vallepu SK, Bayoju K, Srinivas D (2021) A secure image steganography using improved Lsb technique and vigenere cipher algorithm. 2021 International conference on artificial intelligence and smart systems (ICAIS). Coimbatore, India, pp 1005–1010. https://doi.org/10.1109/ICAIS50930.2021.9395794
14. Harjo B, Ignatius Moses Setiadi DR (2021) Improved color image encryption using hybrid modulus substitution cipher and chaotic method. Int J Intell Eng Syst 14:157–166. https://doi.org/10.22266/ijies2021.0430.14
15. Jarjar M et al (2022) New technology of color image encryption based on chaos and two improved Vigenère steps. Multimed Tools Appl 81(17):24665–24689
16. Bagane P et al (2024) Securing data in images using cryptography and steganography algorithms. Int J Intell Syst App Eng 12(15s):17–25
17. Yan S, Wang J, Li L (2024) A color image encryption scheme based on cellular neural networks and linear feedback shift registers. Phys Scr 99(3):035212
18. Islam Y, Li C, Sun K et al (2024) Enhancing image security through an advanced chaotic system with free control and zigzag scrambling encryption. Multimed Tools Appl. https://doi.org/10.1007/s11042-024-18107-0
19. Moumen A, Sissaoui H (2017) Images encryption method using steganographic LSB method, AES and RSA algorithm. Nonlinear Eng 6(1):53–59. https://doi.org/10.1515/nleng-2016-0010
20. Singh S, Attri V (2015) Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm. Int J Signal Process Image Process Pattern Recognition 8:259–266
21. Christy Atika S, EkoHari R, Edi Jaya K (2019) Good performance images encryption using selective bit t-des on inverted lsb steganography. Jurnal Ilmu Komputer dan Informasi 12(1):41–49
22. Durdu A (2024) Image transfer with secure communications application using a new reversible chaotic image encryption. Multimed Tools Appl 83(2):3397–3424
23. Wen H et al (2024) Security analysis of a color image encryption based on bit-level and chaotic map. Multimed Tools Appl 83(2):4133–4149
24. Wen H, Lin Y (2024) Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Syst Appl 237:121514

25. Chen R et al (2024) An image encryption algorithm based on the LSCMM chaotic map and bidirectional dynamic diffusion. Multimed Tools Appl 83(2):3681–3706
26. Toktas A et al (2024) A robust bit-level image encryption based on Bessel map. Appl Math Comput 462:128340
27. Nag A et al (2011) Image encryption using affine transform and XOR operation. 2011 International conference on signal processing, communication, computing and networking technologies. Thuckalay, India, pp 309–312. https://doi.org/10.1109/ICSCCN.2011.6024565
28. Wulandari S (2020) Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message. Proc Int Conf Sci Eng 3:741–744
29. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8:1–35
30. Johnson NF, Jajodia S (1998) Exploring steganography: Seeing the unseen. Computer 31(2):26–34
31. Sadek MM, Khalifa AS, Mostafa MGM (2015) Video steganography: a comprehensive review. Multimed Tools Appl 74:7063–7094. https://doi.org/10.1007/s11042-014-1952-z
32. Pan J, Tompkins WJ (1985) A real-time QRS detection algorithm. IEEE Trans Biomed Eng BME-32(3):230–236
33. Wang X, Du X (2022) Chaotic image encryption method based on improved zigzag permutation and DNA rules. Multimed Tools Appl 81:1–27
34. Showkat E, Sodhi D (2023) Image enhancement in wavelet domain using histogram equalization and median filters. Int J Innov Res Comput Sci Technol 11:25–31
35. Katoch S, Chauhan SS, Kumar V (2021) A review on genetic algorithm: past, present, and future. Multimed Tools Appl 80(5):8091–8126
36. Abdullah H, Enayatifar R, Lee M (2012) A hybrid genetic algorithm and chaotic function model for image encryption. AEU-Int J Electron C 66:806–816
37. Khan M, Masood F (2019) A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimed Tools Appl 78:1–20
38. Wu J, Liao X, Yang B (2018) Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process 153:11–23. https://doi.org/10.1016/j.sigpro.2018.06.008
39. Khan M et al (2021) An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial. Complex Intell Syst 7(5):2751–2764
40. Alexan W, ElBeltagy M, Aboshousha A (2022) Rgb image encryption through cellular automata, s-box and the lorenz system. Symmetry 14(3):443
41. Liu Z et al (2019) A color image encryption using dynamic DNA and 4-D memristive hyper-chaos. IEEE Access 7:78367–78378
42. Kang S et al (2019) Color image encryption method based on 2D-variational mode decomposition. Multimed Tools Appl 78(13):17719–17738
43. Tanveer M et al (2021) Multi-images encryption scheme based on 3D chaotic map and substitution box. IEEE Access 9:73924–73937. https://doi.org/10.1109/ACCESS.2021.3081362
44. Li P, Zhao Y (2017) A simple encryption algorithm for quantum color image. Int J Theor Phys 56(6):1961–1982
45. EtemadiBorujeni S, Eshghi M (2013) Chaotic image encryption system using phase-magnitude transformation and pixel substitution. Telecommun Syst 52(2):525–537
46. Mittal H et al (2022) A comprehensive survey of image segmentation: clustering methods, performance parameters, and benchmark datasets. Multimed Tools Appl 81(24):35001–35026
47. Khalaf A (2016) Fast image encryption based on random image key. https://doi.org/10.13140/RG.2.1.3107.4327
48. Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A (2023) Color image encryption through chaos and KAA map. IEEE Access 11:11541–11554. https://doi.org/10.1109/ACCESS.2023.3242311
49. Sangavi V, Thangavel P (2019) An Image Encryption Algorithm Based On Fractal Geometry. Procedia Comput Sci 165:462–469
50. Kunhoth J et al (2023) Video steganography: recent advances and challenges. Multimed Tools Appl 82(27):41943–41985
51. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. I J Bifurcat Chaos 16:2129–2151
52. Muthukumar P, Khan N (2023) The large key space image encryption algorithm based on modulus synchronization between real and complex fractional-order dynamical systems. Multimed Tools Appl 82(12):17801–17825
53. Wang X, Zhu X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Opt Lasers Eng 107:370–379. https://doi.org/10.1016/j.optlaseng.2017.06.015

54. Curiac D-I, Volosencu C (2012) Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest. Math Probl Eng 2012:940276
55. Kanwal S et al (2021) Analytic study of a novel color image encryption method based on the chaos system and color codes. Complexity 2021:5499538
56. Fu C et al (2018) A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy. Security and Communication Networks 2018:2708532
57. Wang Y, Wu C, Kang S et al (2020) Multi-channel chaotic encryption algorithm for color image based on DNA coding. Multimed Tools Appl 79:18317–18342. https://doi.org/10.1007/s11042-020-08742-8
58. Hardoon DR, Szedmak S, Shawe-Taylor J (2004) Canonical correlation analysis: An overview with application to learning methods. Neural Comput 16(12):2639–2664
59. Shahna KU, Mohamed A (2021) Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion. Signal Process: Image Commun 99:116495
60. Hosny KM, Kamal ST, Darwish MM (2022) A color image encryption technique using block scrambling and chaos. Multimed Tools Appl 81:505–525. https://doi.org/10.1007/s11042-021-11384-z
61. He Y, Li P, Wang X-Y (2020) A new color image encryption scheme based on 2DNLCML system and genetic operations. Opt Lasers Eng 128:106040
62. Shah T, Haq TU, Farooq G (2020) Improved SERPENT algorithm: Design to RGB image encryption implementation. IEEE Access 8:52609–52621
63. Sahu AK, Swain G (2019) An optimal information hiding approach based on pixel value differencing and modulus function. Wireless Pers Commun 108(1):159–174
64. Rafrastara FA, Vega Hadinata A, Ignatius Moses Setiadi DR, Hari Rachmawanto E, Sari CA (2019) Copyright embedding analysis in color image channel based on non-blind DCT method. In: 2019 International conference on information and communications technology (ICOIACT). Yogyakarta, Indonesia, pp 185–190. https://doi.org/10.1109/ICOIACT46704.2019.8938427
65. Wang X et al (2019) A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. Nonlinear Dyn 95:1–28
66. Liao X et al (2023) FAMM: Facial muscle motions for detecting compressed deepfake videos over social networks. IEEE Trans Circuits Syst Video Technol 33:7236–7251
67. Tan J, Liao X, Liu J, Cao Y, Jiang H (2022) Channel attention image steganography with generative adversarial networks. IEEE Transactions on Network Science and Engineering 9(2):888–903. https://doi.org/10.1109/TNSE.2021.3139671
68. Yang Y-G et al (2016) Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. Sci Rep 6(1):19788
69. Kadian K, Garhwal S, Kumar A (2021) Quantum walk and its application domains: A systematic review. Comput Sci Rev 41:100419
70. Cao W-F et al (2018) Constructing quantum Hash functions based on quantum walks on Johnson graphs. Quantum Inf Process 17:1–11

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Ayşegül İhsan[1] · **Nurettin Doğan**[2]

✉ Nurettin Doğan
ndogan@ymail.com

Ayşegül İhsan
aysegulihsann@gmail.com

[1] Department of Information Technologies Engineering, Graduate School of Natural and Applied Sciences, Selçuk University, Alaeddin Keykubat Campus, Konya 42075, Türkiye

[2] Selcuk University, Department of Computer Engineering, Faculty of Technology, Allaeddin Keykubat Campus, Konya 42075, Türkiye