Optimation of image encryption using fractal Tromino and polynomial Chebyshev based on chaotic matrix

Elkaf Rahmawan Pramudya[1,2], Moch Arief Soeleman[1,2], Cahaya Jatmoko[1,2], Eko Hari Rachmawanto[1,2], Aris Marjuni[1,2], Pulung Nurtantio Andono[1,2], Folasade Olubusola Isinkaye[3]
[1]Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia
[2]Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro, Semarang, Indonesia
[3]Department of Computer Science, Faculty of Science, Ekiti State University, Ado-Ekiti, Nigeria

Article Info

Article history:

Received Feb 16, 2024
Revised Jun 11, 2024
Accepted Aug 30, 2024

Keywords:

Encryption quality
Fractal Tromino
Image encryption
Polynomial Chebyshev
Substitution S-box

ABSTRACT

Image encryption is a critical process aimed at securing digital images, safeguarding them from unauthorized access, tampering, or viewing to ensure the confidentiality and integrity of sensitive visual information. In this research, we integrate polynomial Chebyshev, fractal Tromino, and substitution S-box methods into a comprehensive image encryption approach. Our evaluation focuses on standardized 256×256-pixel images of Lena, Peppers, and Baboon, assessing key performance metrics like mean squared error (MSE), peak signal-to-noise ratio (PSNR), unified average changing intensity (UACI), number of pixel changes rate (NPCR), and entropy. The results reveal varying encryption quality across images, with Lena exhibiting the highest MSE (4702) and the lowest PSNR (12.89 dB). However, UACI, NPCR, and entropy values remain consistent across all images, indicating the proposed method's stability concerning changing intensity, pixel alterations, and entropy levels. These findings contribute valuable insights into the effectiveness of the proposed encryption method, providing a foundation for further exploration and optimization in the field of cryptographic research. For future research direction, it is recommended to explore the impact of varying image sizes and types on the proposed method's performance. Additionally, by focusing on the area of cryptographic threats, further analysis of the algorithm's resistance against advanced attacks and its computational efficiency would be beneficial.

Corresponding Author:

Moch Arief Soeleman
Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro
Imam Bojol 207, Semarang, Central Java, 50131, Indonesia
Email: m.arief.soeleman@dsn.dinus.ac.id

1. INTRODUCTION

Image encryption is a process of securing digital images to protect them from unauthorized access, modification, or viewing. This is typically done to ensure the confidentiality and integrity of sensitive visual information [1], [2]. Implementation of various cryptographic techniques and algorithms, image encryption transforms digital images into obscured formats, making it challenging for unauthorized entities to decipher or manipulate the original content [3], [4]. This protective measure plays a vital role in diverse fields where the privacy and security of visual data are paramount. The essence of image encryption lies in the utilization of a 'key', a confidential parameter that must remain undisclosed to unauthorized individuals [5]. This key serves as a critical element in the encryption process, ensuring that only those with the correct key can decrypt and access the original visual content [6]-[8]. The security of the encrypted images hinges on the secrecy of this key, emphasizing the need for robust key management practices. By restricting knowledge of the key to authorized parties, the encryption mechanism establishes a protective barrier, fortifying the confidentiality of sensitive visual information against potential breaches. This stringent control over access to the decryption key is paramount in upholding the overall security and effectiveness of image encryption techniques [9]. Based on the review, the evolution of image encryption techniques by [8]-[14] has been shaped by ongoing advancements in cryptographic research and technology. Researchers and practitioners continually explore novel approaches to enhance the resilience of image encryption against evolving cyber threats. Recent developments have seen the integration of machine learning algorithms to reinforce encryption processes, providing an additional layer of defense against sophisticated attacks [15]. The intersection of image encryption with other cybersecurity measures, such as secure transmission protocols and multi-factor authentication, contributes to creating a comprehensive and robust security framework for visual data [16], [17]. Moreover, the adoption of quantum-resistant encryption algorithms is gaining attention as a proactive measure to address the potential vulnerabilities posed by quantum computing in the future. In addition to technological advancements, the widespread adoption of image encryption standards and protocols further underscores its significance. Industry-wide acceptance of standardized encryption practices ensures interoperability and facilitates seamless collaboration across different platforms and applications. Standardization not only enhances the compatibility of image encryption solutions but also fosters trust among users by adhering to established security benchmarks. Collaborative efforts among researchers, industry stakeholders, and policymakers are instrumental in developing and promoting these standards, fostering a more secure digital landscape.

The primary aim of this research is to advance the quality measurement techniques for image encryption through the integration of innovative methodologies, specifically employing the fractal Tromino and polynomial Chebyshev transformations based on chaotic matrices. The goal is to enhance the precision and reliability of quality metrics such as the mean squared error (MSE), peak signal-to-noise ratio (PSNR), number of pixel changes rate (NPCR), and unified average changing intensity (UACI) in assessing the effectiveness of image encryption algorithms. By leveraging the unique properties of fractal Tromino and polynomial Chebyshev transformations within the framework of chaotic matrices, the research seeks to develop a more robust and sensitive quality measurement mechanism. This approach aims to provide a comprehensive evaluation of the encryption algorithms, offering insights into their capacity to induce significant pixel changes and alterations across images while maintaining the desirable properties of encryption, such as confidentiality and resistance against unauthorized access.

This research is structured to comprehensively explore and enhance quality measurement in image encryption, leveraging the innovative integration of fractal Tromino and polynomial Chebyshev transformations within the framework of chaotic matrices. Section 1 introduces the problem of securing digital images and the importance of robust encryption methods, providing a background on existing approaches and their limitations. Section 2 presents a detailed literature review on current encryption techniques, particularly focusing on chaos-based encryption, fractal geometry, and polynomial transformations. In section 3, the proposed method is discussed, outlining the integration of fractal Tromino and polynomial Chebyshev transformations within chaotic matrices, explaining how this combination improves encryption quality and security. Section 4 analyzes the results obtained from implementing the proposed method, evaluating its performance using metrics such as PSNR, SSIM, entropy, and comparing it to traditional methods. Finally, section 5 concludes the research by summarizing the findings, highlighting the improvements achieved, and suggesting future work.

2. LITERATURE REVIEW

2.1. State of the art

The utilization of fractal Tromino and polynomial Chebyshev in the context of image encryption is relatively uncommon. However, a discernible number of research studies have demonstrated the efficacy of employing either one of these methods as part of their image encryption strategies. Moreover, some researchers have taken an innovative approach by combining these less conventional techniques with other established methods to enhance the overall security and robustness of their data protection mechanisms.

The research, as represented by [18], introduces a novel approach to ensure highly secure data transmission through the proposition of a hybrid encryption technique. In this method, encryption and decryption processes are intricately designed by incorporating a hybrid fractal-chaos technique, which comprises four essential modules: key generation, fractal encryption, chaos encryption, and decryption. Initially, a generated key is employed to facilitate both the encryption and decryption of images or data. Subsequently, the fractal encryption process is executed through the application of the L-shaped Tromino. Simultaneously, chaos encryption is carried out using the discrete cosine transform (DCT), culminating in the production of the final encrypted image. The decryption process involves the utilization of chaos decryption and fractal decryption algorithms. Research by Khan *et al.* [19], proposed encryption scheme is built upon a foundation of fractal Tromino and a Chebyshev polynomial-based generated chaotic matrix. The scheme prioritizes two fundamental aspects of encryption: diffusion and confusion. To achieve confusion, highly non-linear, pre-defined S-boxes are strategically incorporated. Rigorous testing of the proposed scheme has been conducted using key performance indicators such as differential analysis, statistical analysis, information entropy analysis, MSE, and NIST-based randomness analysis. The findings reveal that the encrypted images exhibit the highest practically achievable entropy of 7.9999. Importantly, the time analysis demonstrates the feasibility of real-time implementation for the proposed system. In the research conducted by [20], the researchers devised an algorithm that combines the digital wavelet transform with fractal encryption to enhance image security. The process initiates with the transformation of a host image into the frequency domain through the discrete wavelet transform. The resulting encrypted watermark is then embedded into the host image in the frequency domain, culminating in the creation of a watermarked image.

The current study adopts a hybrid approach by incorporating elements of the proposed method, specifically integrating the innovative techniques of fractal Tromino and polynomial Chebyshev. This novel combination aims to further enhance the encryption process, leveraging the unique properties of each method to fortify the security measures employed. The forthcoming section will delve into a detailed exploration of the application and intricacies of the fractal Tromino and polynomial Chebyshev methods within the context of this research, elucidating their roles in optimizing image encryption and contributing to the overall efficacy of the proposed algorithm. By synergizing these methods, the study aims to provide a comprehensive understanding of their collective impact on image security, thereby advancing the current state-of-the-art cryptographic practices.

2.2. Substitution S-box

Substitution S-boxes are integral components in cryptographic systems, particularly block ciphers [21], [22]. Their primary function is to facilitate the nonlinear transformation of input data during the encryption process, contributing significantly to the overall security of the algorithm. The substitution of values within these boxes introduces a layer of confusion and diffusion, thereby complicating the ability of adversaries to discern patterns or relationships between the plaintext and ciphertext. Pseudocode-based S-boxes substitution logic can be seen in Algorithm 1. The provided S-box substitution algorithm employs a predefined substitution table, $S-box\_table$, to substitute input bytes. The algorithm ensures that the $input\_byte$ is within a valid range (0 to 255) by applying the modulo operation with 256. This modular operation is represented by (1), where mod denotes the modulo operation. This equation ensures that the $input\_byte$ remains within the valid byte range, preventing overflow. The algorithm then proceeds to substitute the $input_byt$e with the corresponding value from the $S-box\_table$, producing the $output\_byte$.

2.3. Fractal Tromino

Fractal Tromino processing involves the recursive application of a mathematical algorithm to create intricate patterns known as fractals, specifically focusing on the construction of a geometric shape known as a Tromino. The Tromino is a type of polyomino consisting of three connected squares [19], [20]. In this process, a base shape, often a single square, is repeatedly divided into smaller Trominos through a set of recursive rules. This recursive subdivision leads to the emergence of self-similar patterns on different scales within the overall structure. Based on the fractal Tromino algorithm, can be seen in Algorithm 2. The fractal Tromino algorithm aims to generate a matrix, denoted as R, from an input image matrix using a series of mathematical operations. The matrix R is constructed through iterations over the dimensions of the input image, incorporating randomly generated keys $k1$ and $k2$ and a computed value c based on the mean of the input image. In (3) illustrates the updating of each element in R by applying a combination of the existing value, $k1$ multiplied by c, and $k2$, followed by modulo 256. The computed value c in (4) and (5) is determined by summing the absolute differences between each element of the input image and its mean, divided by the product of the image dimensions. The final step involves performing an XOR operation in (6) between the original image and the generated fractal Tromino, resulting in a modified image, referred to as the $resulting\ image$.

2.4. Polynomial Chebyshev based on chaotix matrix processing

Polynomial Chebyshev based on chaotix matrix processing in cryptography refers to a novel approach that integrates Chebyshev polynomials with the concept of chaotix matrices for enhancing cryptographic operations [19], [23]. Chaotix matrices are characterized by their chaotic and unpredictable properties, and when combined with the mathematical elegance of Chebyshev polynomials, they provide a platform for creating robust cryptographic protocols. The synergy of Chebyshev-based polynomial processing and chaotix matrices can be leveraged for tasks such as secure key generation, encryption, and authentication. Based on the Polynomial Chebyshev equation can be seen in (7). The provided algorithm outlines a Chebyshev-based image-processing function in cryptography. The algorithm initializes keys p and q along with a constant c derived from the input image matrix as shown in Algorithm 3. It then iteratively updates a matrix R based on conditional rules involving $k1$ and $k2$. Subsequently, Chebyshev polynomials are applied to update p and q in a nested loop that runs for $M * N$ iterations, where M and N are the dimensions of the image. Two matrices, $matrix1$, and $matrix2$, are generated by processing p and q using a modulus operation. The final result is obtained by XORing these matrices.

Algorithm 1. S-boxes substitution algorithm

```
**Function** $SubstitutionSBox\ (input\_matrix)$:
    M, N = $size(input\_matrix)$
    binMat = convertToBinary $(input\_matrix, M, N)$
    partitioned = partitionMatrix $(binMat, M, N)$
    for $i$ from 1 to $M$:
        for $j$ from 1 to $N$:
            partitioned $[i, j]$ = SubByte (partitioned $[i, j]$)
    reassembled = reassemble at $(partitioned,\ M, N)$
  return $reassembled$
**End**
**Function** $SubByteOperation\ (partition)$:
  for $i$ from 1 to size $(partition, 1)$:
    for $j$ from 1 to size $(partition, 2)$:
  partition $[i, j]$ = SboxSubstitution (partition$[i, j]$)
  return $partition$
**End**
**Function** $Substitution(input\_byte)$:
  $S - box\_table$ = [
    0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F
    0x30, 0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB
    0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47
    0xAD, 0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72]
    $input\_byte\ =\ input\_byte\ mod\ 256$        (1)
  $output_{byte}\ =\ S - box_{table}$
                                              $[input\_byte]$
  return $output\_byte$
**End**
```

Algorithm 2. Fractal Tromino algorithm

```
**Function** $generateFractalTromino(imageMatrix)$:
  $M, N, \_$ = $size\ (imageMatrix)$
  $R$ = $createMatrix\ (M, 3\ *\ N)$
  $k1, k2$ = $generateRandomKey$ ()
  $m$ = $mean(imageMatrix)$
  for $i$ from 1 $to$ $M$:
    for $j$ from 1 $to$ $3\ *\ N$:
      $c$ = $computeC\ (imageMatrix, m)$
      $R\ [i, j]\ =\ (R\ [i, j]\ +\ k1\ *\ c\ +\ k2)\ \%\ 256$   (3)
   $fractalTromino$ = $reshapeMatrix\ (R, M, N, 3)$
   return $fractalTromino$
**End**
**Function** $computer(matrix, mean)$:
  $sum\ =\ 0$
  for each element in the matrix:
   sum = $sum\ +\ abs\ (element\ -\ mean)$               (4)
   $c = round(sum/(size(matrix, 1$                       (5)
                    $* size(matrix, 2)))$
  return $c$
**End**
**Function** $generateRandomKey$ ():
  return $randomInteger(0, 255)$
End
Function $xorWithFractal\ (orimage, fractalTromino)$:
  resultImage =                                    (6)
  $oriImage\ XOR\ fractalTromino$
  return $resultImage$
End
```

Algorithm 3. Polynomial Chebyshev algorithm

```
Function $Chebyshev\ (imageMatrix, x, y, k1, k2)$:
  M, N = $size\ (imageMatrix)$
  p = $initializeKey$ ()
  q = $initializeKey$ ()
  c = $calculateC\ (imageMatrix)$
  for $i$ from 1 $to\ M$:
    for $j$ from 1 $to\ N$:
      if $mod\ (i, k2 * c) < k1 * c$:
        $R[i, j] = mod(j, r)$
      elseif $mod\ (j, k2 * c) > k1 * c$:
        $R[i, j] = mod(i, r)$
      else:
        $R[i, j] = mod(c - i, c)$
  for iteration from 1 to $M * N$:
    p = $cos\ (x * arccos\ (w * p))$
    $q = cos(y * arccos(q))$
  matrix1 = $processMatrix(p, q, M, N, r)$
  matrix2 = $processMatrix(q, p, M, N, r)$
  resultMatrix = $matrix1\ XOR\ matrix2$
  return $resultMatrix$
End
```

$$p(k+1) = Tn(pk) = cos(x \times arccos(wk)) \qquad (7)$$
$$q(l+1) = Tm(ql) = cos(y \times arccos(ql)),$$

2.5. Quality measuremet

MSE is a widely used metric in cryptography to quantify the difference between an original image and its reconstructed or encrypted version [24], [25]. The MSE is calculated by taking the average of the squared differences between corresponding pixel values in the two images. The equation for MSE based on grayscale images can be seen in (8). Where M and N represent the dimensions of the images, I_{ij} denotes the pixel intensity of the original image, and K_{ij} is the pixel intensity of the encrypted or reconstructed image. A lower MSE value indicates a closer match between the two images, implying a smaller difference between the original and the encrypted image. If MSE approaches 0, it signifies that the encrypted image is nearly identical to the original, suggesting a successful and accurate encryption process. On the other hand, an MSE value approaching 1 implies a significant deviation between the original and encrypted images, indicating a higher level of distortion or error in the encryption process [5]. In summary, a lower MSE is desirable as it reflects a higher fidelity in preserving the content of the original image during encryption, while a higher MSE indicates greater distortion. For red, green, and blue (RGB) images, the MSE calculation is performed independently for each color channel, and the final MSE is the average of the MSE values for each channel. The equation for MSE based on RGB images can be seen in (9). PSNR is especially relevant in cryptography when assessing the fidelity of encrypted images [26]. The PSNR is calculated as the ratio of the peak signal value to the MSE between the original and encrypted images, expressed in decibels (dB). The equation for PSNR can be seen in (9).

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - K(i,j)\right)^2 \qquad (8)$$

$$MSE = \frac{1}{3MN}\sum_{k=1}^{3}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j,k) - K(i,j,k)\right)^2 \qquad (9)$$

$$PSNR = 10\log 10\left(\frac{\max\_pixel\_value^2}{MSE}\right) \tag{10}$$

UACI is a metric used to assess color distortion in image or video processing applications [23]. A high UACI value indicates a significant chromaticity change between the original and processed images, reflecting a substantial alteration in color information. On the contrary, a low UACI value signifies minimal chromaticity change, indicating that the processed image closely preserves the original color information. The equation based on UACI can be seen in (11):

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) \oplus K(i,j)}{L}\right| \times 100 \tag{11}$$

NPCR is a quality measurement metric employed in image processing to assess the effectiveness of cryptographic algorithms by quantifying the extent of pixel change between an original and an encrypted image [27]. A higher NPCR value signifies that a larger proportion of pixels experience changes, indicating a greater sensitivity to alterations in the encryption key. In contrast, a lower NPCR value indicates that fewer pixels are affected by changes in the encryption key. The equation based on NPCR can be seen in (12). Where, M and N represent the dimensions of the images, $I(i,j)$ denotes the pixel intensity of the original image at coordinates (i,j). $K(i,\, j)$ is the pixel intensity of the processed or encrypted image at the same coordinates, and L signifies the maximum pixel intensity value. The formula computes the average percentage change in chromaticity between corresponding pixels in the original and processed images, with the XOR ($\oplus$) operation used to calculate the bitwise exclusive OR of the pixel intensities. The resulting values are normalized by L and multiplied by 100 to express the percentage change.

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) - K(i,j)}{I(i,j)}\right| \times 100 \tag{12}$$

Entropy is a statistical measure used in information theory and image processing to quantify the randomness or unpredictability of pixel intensities within an image. In the context of image analysis, entropy represents the level of disorder in the pixel values entropy indicates greater disorder, complexity, and information content, while lower entropy suggests a more ordered and predictable image. A high entropy value implies that the image contains a wide range of pixel intensity values and lacks a discernible pattern, making it more challenging to predict or compress. Based on entropy equation can be seen in (13):

$$Entropy = -\sum_{i=1}^{n} P(x_i) \cdot Log_2(P(x_i)) \tag{13}$$

3. PROPOSED SCHEME

The proposed scheme involves a combination of substitution S-box, fractal Tromino, and polynomial Chebyshev algorithms for encryption. The encryption process is outlined:

- Step 1: substitution S-box initialization. Convert the input image matrix into binary form and partition it. Apply the SubByte operation using S-box substitution for each partition.
- Step 2: fractal Tromino initialization. Create a matrix R based on the image dimensions. Generate random keys $k1$ and $k2$, calculate c using (5), and update R using (3).
- Step 3: Chebyshev initialization. Initialize keys p and q, calculate c and update matrix R based on conditional rules.
- Step 4: fractal Tromino processing. Generate fractal Tromino using the initialized matrix R and random keys $k1$ and $k2$.
- Step 5: Chebyshev processing. Iterate through Chebyshev processing on the image matrix using keys $p, q, x, y, k1$, and $k2$. This involves applying Chebyshev polynomials and updating matrix R.
- Step 6: substitution S-box processing. Perform substitution S-box operation on the encrypted matrix obtained from the fractal Tromino and Chebyshev processing.
- Step 7: XOR operation. XOR the results obtained from fractal Tromino and Chebyshev processing to generate the final encrypted matrix.
- Step 8: output. The encrypted image is obtained as the result of the XOR operation.

Based on steps 1 to 8, the aforementioned process is visually represented in Figure 1, offering a comprehensive illustration of each stage in the encryption workflow as in Figure 1. Based on the fractal Tromino algorithm and Figure 2, the visual depiction clearly illustrates a sequence of steps through a series of processes outlined:

- Step 1: the process begins by sampling the initialized image, typically represented as a matrix of dimensions $M \times N \times 3$ (height, width, and color channels). Subsequently, two random keys $k1$ and $k2$ are generated using the generateRandomKey function. The mean (m) of the image matrix is computed through the mean (imageMatrix).
- Step 2: for each pixel in the initialized image, the algorithm undergoes $M \times 3N$ iterations. The computation of c is executed using the computeC ($matrix, mean$) function, involving the summation of absolute differences between each matrix element and the mean, as defined in (4). The computed c is then employed to update the fractal matrix R using (3).
- Step 3: the resultant matrix R is reshaped into a $M \times N \times 3$ matrix to yield the fractal Tromino. This generated fractal Tromino is subsequently returned.
- Step 4: the final step entails XORing the acquired fractal Tromino with the RGB image using the xorWithFractal (oriImage and fractalTromino) function and (6). This XOR operation finalizes the encryption process.

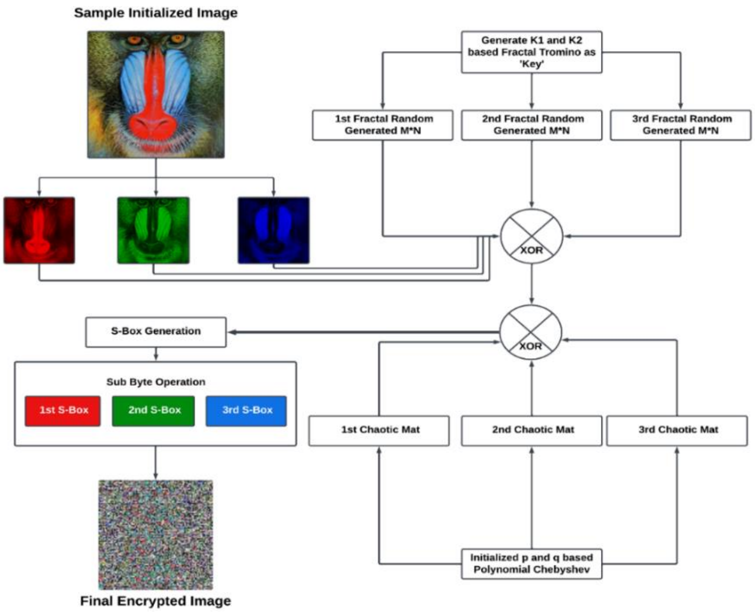
Sample Initialized Image
Generate K1 and K2 based Fractal Tromino as 'Key'
1st Fractal Random Generated M*N
2nd Fractal Random Generated M*N
3rd Fractal Random Generated M*N
XOR
XOR
S-Box Generation
Sub Byte Operation
1st S-Box
2nd S-Box
3rd S-Box
1st Chaotic Mat
2nd Chaotic Mat
3rd Chaotic Mat
Initialized p and q based Polynomial Chebyshev
Final Encrypted Image

Figure 1. Proposed encryption scheme

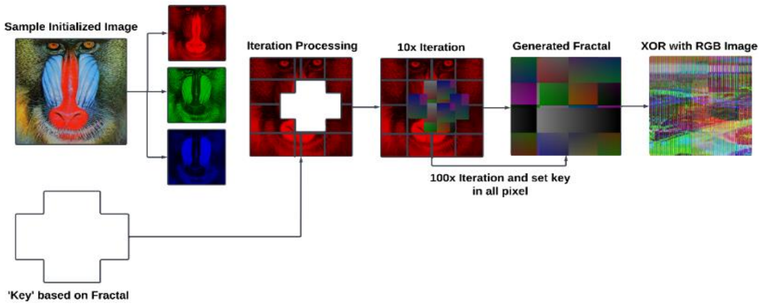

Figure 2. Visualization of fractal processing

4. RESULTS AND DISCUSSION

In this experiment, the proposed image encryption method was implemented on a dedicated device with specifications including an Intel Core i7 10th Gen processor, RTX 3050 graphics card, 16 GB RAM, and a 256 GB SSD. The software execution was carried out using MATLAB 2021b. The dataset employed for this research consisted of PNG images widely used in related studies, namely Lena, Peppers, and Baboon. The visual representation of these images is depicted in Figures 3(a)–(d). As illustrated in Figures 3(a)–(d), the outcomes of the image processing procedure revealed distinct transformations in the Lena, peppers, and Baboon images. After the application of the proposed fractal Tromino-based image encryption algorithm, the processed images are visually represented in Figures 4(a)–(d). The testing phase, as depicted in Figures 4(a)–(d), presents a comprehensive evaluation of the proposed image encryption algorithm. The encrypted counterpart is featured in Figure 4(c), providing a visual insight into the transformation induced by the fractal Tromino-based encryption. To quantitatively assess the fidelity of the encrypted image, MSE and PSNR metrics were computed and are visually represented in Figures 5 and 6, respectively.

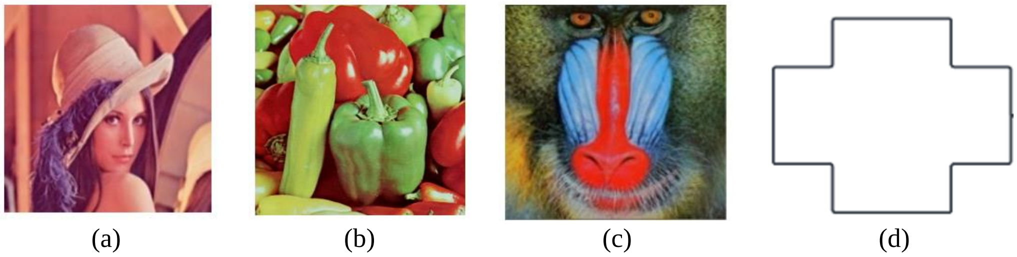

Figure 3. Sample image datasets; (a) Lena.png, (b) Peppers.png, (c) Baboon.png, and key for fracta

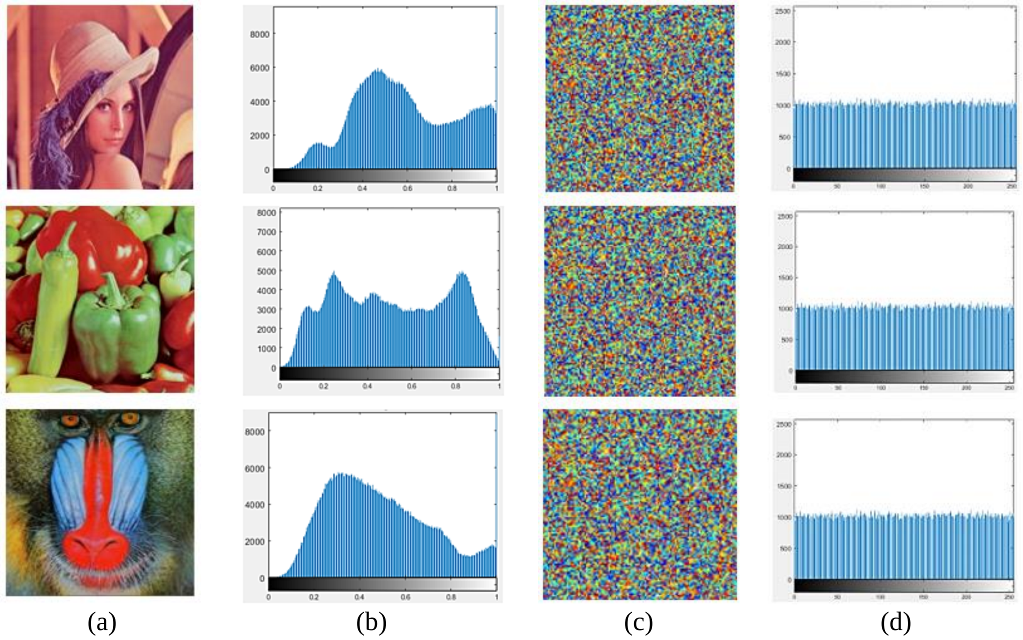

Figure 4. Testing phase; (a) original image, (b) histogram based original image, (c) encrypted image, and (d) histogram based encrypted image

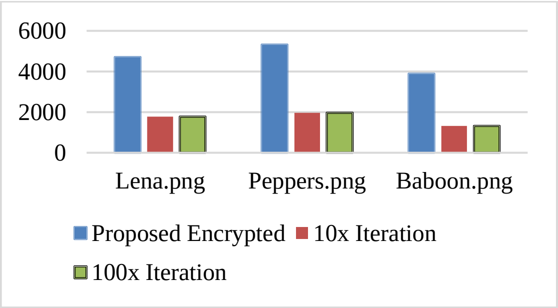

Figure 5. Comparison based on MSE

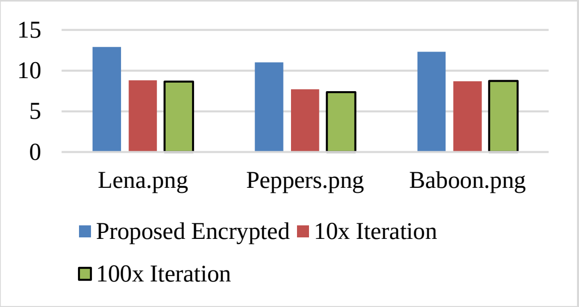

Figure 6. Comparison based on PSNR

Figures 7(a)–(d) provides a comprehensive visual representation of the MSE and PSNR metrics across two significant iteration counts, namely 10× and 100×. The iterative nature of the proposed fractal Tromino-based image encryption algorithm is explored to understand its impact on the quality of encryption. The MSE and PSNR values are depicted in Figures 5 and 6, portray the evolution of dissimilarity between the original and encrypted images as the iteration count increases. In Figure 7(d), the visual representation encapsulates the essence of the proposed method, which amalgamates the distinctive attributes of the fractal Tromino algorithm, polynomial Chebyshev processing, and substitution S-box.

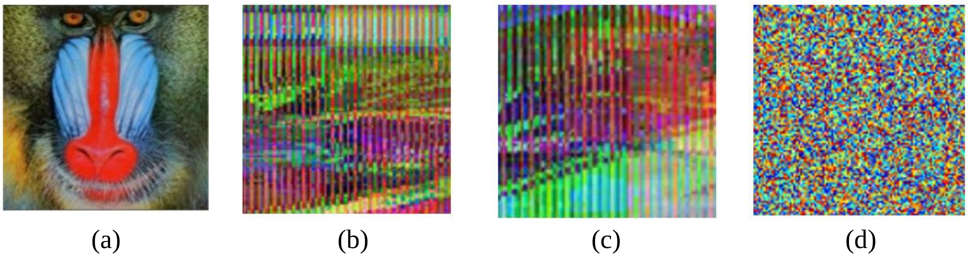

Figure 7. Comparison results visualization; (a) tested image Baboon.png, (b) tested with 10× iteration, (c) tested with 100× iteration, and (d) proposed method

In a histogram, the horizontal axis (x-axis) represents the intensity values or brightness levels of an image. These values typically range from 0 to 255 in grayscale images, where 0 corresponds to black, 255 corresponds to white, and the values in between represent various shades of gray. For colored images, the intensity values for each color channel (red, green, and blue) are represented similarly. Meanwhile, the vertical axis (y-axis) indicates the frequency or the number of occurrences of each intensity value in the image. This frequency shows how many pixels in the image correspond to each specific intensity level, providing a clear representation of the image's overall contrast and brightness distribution.

Another test using UACI and NPCR provides additional insights into the proposed image encryption method. This evaluation is complemented by a comparative analysis with relevant studies, as outlined in Table 1. The juxtaposition of these findings with those from related studies enables a comprehensive assessment of the proposed method's efficacy in terms of pixel-level alterations and overall intensity changes. The comparative analysis presented in the table highlights the performance of the proposed image encryption method in contrast to several existing studies, as measured by the UACI and the NPCR. In terms of UACI, the proposed method demonstrates a value of 33.48, indicating the average changing intensity across encrypted images. This places it near the results obtained by Alghafis *et al*. [27], Khan *et al*. [28], He *et al*. [29], and Norouzi and Mirzakuchaki [30], where UACI values range from 33.44 to 33.50. On the NPCR front, the proposed method achieves a rate of 99.66%, outperforming the counterparts mentioned in the comparison. Khan *et al*. [19] closely trails the proposed method with a rate of 99.64%, while the others range from 99.57% to 99.63%. The final assessment involves computing the entropy of the encrypted images as a comprehensive measure of information content. Entropy, depicted in Table 1, serves as an essential metric to evaluate the randomness and uncertainty within the encrypted images. Based on the comprehensive quality measurements presented in Table 1, which focus on three benchmark images—Lena, Peppers, and Baboon—the optimal outcomes from each image are compiled in Table 2. The outcomes derived from the comprehensive evaluation presented in Table 2 offer a detailed assessment of the proposed method's performance, considering image datasets standardized to a size of 256×256×3.

Table 1. UACI and NPCR measurement

Research	UACI (%)	NPCR (%)	Entropy
Khan *et al*. [28]	33.46	99.63	7.9970
Alghafis *et al*. [27]	33.45	99.57	7.9970
He *et al*. [29]	33.44	99.62	7.9999
Norouzi and Mirzakuchaki [30]	33.50	99.62	7.9980
Khan *et al*. [19]	33.47	99.64	7.9999
Proposed Method	33.48	99.66	7.9999

Table 2. Value information based on the testing phase

Sample image	MSE	PSNR	UACI	NPCR	Entropy
Lena.png	4702	12.89 dB	33.48	99.66	7.9999
Peppers.png	5321	11.12 dB	33.48	99.65	7.9999
Baboon.png	3894	12.31 dB	33.46	99.65	7.9999

5. CONCLUSION

The testing phase results reveal crucial insights into the performance of the proposed image encryption method across various sample images, namely Lena, Peppers, and Baboon, each standardized to a size of 256×256 pixels with three color channels. The MSE values, representing the average squared differences between the original and encrypted images, indicate that Lena has the highest MSE (4702), followed by Peppers (5321) and Baboon (3894). PSNR, a measure of image quality, exhibits corresponding trends, with Lena having the lowest PSNR (12.89 dB), followed by Peppers (11.12 dB) and Baboon (12.31 dB). UACI and NPCR show consistent values across all three images, emphasizing the stability of the proposed method. The entropy values remain constant at 7.9999 for all images, denoting a consistent level of disorder in the encrypted data. Overall, these quantitative metrics provide a comprehensive evaluation of the proposed method's efficacy in securing image data, considering both visual fidelity and encryption robustness. This research has laid a foundation for the integration of fractal tromino, polynomial Chebyshev, and substitution S-box methods in image encryption, showcasing promising results in terms of MSE, PSNR, UACI, NPCR, and entropy. For future endeavors, it is recommended to explore the impact of varying image sizes and types on the proposed method's performance. Additionally, considering the evolving landscape of cryptographic threats, further analysis of the algorithm's resistance against advanced attacks and its computational efficiency would be beneficial. Exploring the integration of other encryption techniques and conducting a comparative study with state-of-the-art methods could provide valuable insights into the proposed method's relative strengths and weaknesses. Furthermore, the research community could delve into optimizing the algorithm for real-time applications and expanding its applicability to diverse multimedia data beyond static images.

ACKNOWLEDGEMENTS

This research is supported by the Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro.

REFERENCES

[1] M. Arora and M. Khurana, "Secure image encryption technique based on jigsaw transform and chaotic scrambling using digital image watermarking," *Optical and Quantum Electronics*, vol. 52, no. 2, Feb. 2020, doi: 10.1007/s11082-019-2130-3.

[2] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[3] Z. A. Abduljabbar *et al.*, "Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.

[4] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019, doi: 10.1007/s41939-019-00049-y.

[5] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568–580, 2023, doi: 10.22266/ijies2023.0831.46.

[6] A. S. D. Alluhaidan and P. Prabu, "End-to-End Encryption in Resource-Constrained IoT Device," *IEEE Access*, vol. 11, pp. 70040–70051, 2023, doi: 10.1109/ACCESS.2023.3292829.

[7] M. Abu-Faraj *et al.*, "Protecting Digital Images Using Keys Enhanced by 2D Chaotic Logistic Maps," *Cryptography*, vol. 7, no. 2, 2023, doi: 10.3390/cryptography7020020.

[8] E. Y. Purba, S. Efendi, P. Sirait, and P. Sihombing, "Collaboration of RSA Algorithm Using EM2B Key with Word Auto Key Encryption Cryptography Method in Encryption of SQL Plaintext Database," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Sep. 2019, doi: 10.1088/1742-6596/1230/1/012009.

[9] F. ElAzzaby, K. H. Sabour, N. ELakkad, W. El-Shafai, A. Torki, and S. R. Rajkumar, "Color image encryption using a Zigzag Transformation and sine–cosine maps," *Scientific African*, vol. 22, Nov. 2023, doi: 10.1016/j.sciaf.2023.e01955.

[10] M. Kaur, S. Singh, and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review," *Mathematical Problems in Engineering*, vol. 2021, 2021, doi: 10.1155/2021/5012496.

[11] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps: Image encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, Mar. 2020, doi: 10.1007/s12652-019-01493-x.

[12] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, P. Kumaresan, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–19, 2020, doi: 10.3390/s20185162.

[13] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25497–25518, Jul. 2022, doi: 10.1007/s11042-022-12595-8.

[14] C.-L. Li, Y. Zhou, H.-M. Li, W. Feng, and J.-R. Du, "Image encryption scheme with bit-level scrambling and multiplication diffusion," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18479–18501, 2021, doi: 10.1007/s11042-021-10631-7.

[15] V. Prabhakaran and A. Kulandasamy, "Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection," *Neural Computing and Applications*, 2021, doi: 10.1007/s00521-021-06085-5.

[16] A. Mozo, A. Karamchandani, L. de la Cal, S. Gómez-Canaval, A. Pastor, and L. Gifre, "A Machine-Learning-Based Cyberattack Detector for a Cloud-Based SDN Controller," *Applied Sciences (Switzerland)*, vol. 13, no. 8, Apr. 2023, doi: 10.3390/app13084914.

[17] M. Wazid, A. K. Das, V. Chamola, and Y. Park, "Uniting cyber security and machine learning: Advantages, challenges and future research," *ICT Express*, vol. 8, no. 3, pp. 313–321, Sep. 01, 2022, doi: 10.1016/j.icte.2022.04.007.

[18] S. R. M. Halagowda and S. K. Lakshminarayana, "Image encryption method based on hybrid fractal-chaos algorithm," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 6, pp. 221–229, 2017, doi: 10.22266/ijies2017.1231.24.

[19] M. Khan, A. S. Alanazi, L. S. Khan, and I. Hussain, "An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial," *Complex and Intelligent Systems*, vol. 7, no. 5, pp. 2751–2764, Oct. 2021, doi: 10.1007/s40747-021-00460-4.

[20] N. S. Awarayi, O. Appiah, B. A. Weyori, and C. B. Ninfaakang, "A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption," *International Journal of Image, Graphics and Signal Processing*, vol. 13, no. 3, pp. 33–43, Jun. 2021, doi: 10.5815/ijigsp.2021.03.03.

[21] S. Chen *et al.*, "SAND: an AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations," *Designs, Codes and Cryptography*, vol. 90, no. 1, pp. 155–198, Jan. 2022, doi: 10.1007/s10623-021-00970-9.

[22] L. Xiao and H. M. Heys, "Software Performance Characterization of Block Cipher Structures Using S-boxes and Linear Mappings," *IEE Proceedings-Communications*, vol. 152, no. 5, pp. 567–579, Oct. 2005, doi: 10.1049/ip-com:20045223.

[23] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[24] N. Mahendiran and C. Deepa, "A Comprehensive Analysis on Image Encryption and Compression Techniques with the Assessment of Performance Evaluation Metrics," *SN Computer Science*, vol. 2, no. 1, 2021, doi: 10.1007/s42979-020-00397-4.

[25] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[26] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications*, vol. 80, no. 6, pp. 8423–8444, Mar. 2021, doi: 10.1007/s11042-020-10035-z.

[27] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, "An efficient image encryption scheme based on chaotic and Deoxyribonucleic acid sequencing," *Mathematics and Computers in Simulation*, vol. 177, pp. 441–466, Nov. 2020, doi: 10.1016/j.matcom.2020.05.016.

[28] S. Khan, L. Han, H. Lu, K. K. Butt, G. Bachira, and N. U. Khan, "A New Hybrid Image Encryption Algorithm Based on 2D-CA, FSM-DNA Rule Generator, and FSBI," *IEEE Access*, vol. 7, pp. 81333–81350, 2019, doi: 10.1109/ACCESS.2019.2920383.

[29] Y. He, Y. Q. Zhang, and X. Y. Wang, "A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system," *Neural Computing and Applications*, vol. 32, no. 1, pp. 247–260, Jan. 2020, doi: 10.1007/s00521-018-3577-z.

[30] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13681–13701, Jun. 2017, doi: 10.1007/s11042-016-3769-4.

BIOGRAPHIES OF AUTHORS

Elkaf Rahmawan Pramudya received a Bachelor's degree in Informatics Engineering in 1996 from the University of Dian Nuswantoro, and a Master's degree from the University of Dian Nuswantoro in 2011. From 2016 to 2022 he was the Lead of the Computer Laboratory of the University of Dian Nuswantoro. Became a lecturer in 1998 with competency in the field of computer networks. Currently joining the research center for intelligent distributed surveillance and security to develop issues regarding data security. He can be contacted at email: elkaf.rahmawan@dsn.dinus.ac.id.

Moch Arief Soeleman received a Bachelor's degree in Informatics Engineering in 1999 and a Master's degree in 2004, respectively from the University of Dian Nuswantoro. Continuing his doctoral education and graduated from the Institute of Technology Sepuluh November in 2016. Now, he is an Associate Professor. Since 2017, he has served as Lead of Study Program in the Master of Informatics Engineering University of Dian Nuswantoro. Research interests in the fields of computer vision and data security. He can be contacted at email: m.arief.soeleman@dsn.dinus.ac.id.

Cahaya Jatmoko received Bachelor's and Master's degrees from the University of Dian Nuswantoro respectively in 2002 and 2011. Has been a lecturer since 2012. Until now, he has been active in researching and giving oral presentations in international conferences and international journals. Research interest include image processing, computer vision, pattern recognition, machine learning, and computing data security. He can be contacted at email: cahayajatmoko@dsn.dinus.ac.id.

Eko Hari Rachmawanto received a Bachelor's degree in Informatic Engineering from the University of Dian Nuswantoro, in 2010. He received a Master's double degree University of Dian Nuswantoro and Universiti Teknikal Malaysia Malacca (UTeM) in 2010 and 2012. Since 2012, he joined as a lecturer in Informatics Engineering at, the University of Dian Nuswantoro, Semarang, Indonesia. Now he serves as Editor in Chief of Accredited Indonesian National Journal. Since 2022 he has supervised the Informatics Engineering study program in study programs outside the main campus as head of the study program in Kediri, Indonesia. Now he is a member of security data collaboration research and tasked with developing several researchers regarding data security, and image processing. He can be contacted at email: eko.hari@dsn.dinus.ac.id.

Aris Marjuni was born in Wonogiri, Central Java, Indonesia, in 1969. He received a Doctoral degree in Electrical Engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2019. He is currently an Associate Professor with the Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Central Java, Indonesia. His research interests include image processing, data mining, software engineering, soft computing, information systems, and statistics. He can be contacted at email: aris.marjuni@dsn.dinus.ac.id.

Pulung Nurtantio Andono received a Bachelor's degree from Trisakti University, Jakarta, Indonesia, in 2006, a master's degree from Dian Nuswantoro University, Semarang, Indonesia, in 2009, and a Ph.D. degree from the Institut Teknologi Sepuluh November (ITS), Surabaya, Indonesia, in 2016. He currently works as a Lecturer and a Researcher at the Faculty of Computer Science, Dian Nuswantoro University. His research interests include image security, computer vision, and 3D image reconstruction. He has authored or co-authored more than 43 refereed journals and conference papers indexed by Scopus. He can be contacted at email: pulung@dsn.dinus.ac.id.

Folasade Olubusola Isinkaye received a Bachelor of Science degree in Computer Science from the Ondo State University, Ado-Ekiti, (now EKSU) Nigeria. Her Master of Science and Ph.D. degrees were obtained in Computer Science from the University of Ibadan, Nigeria. She is a Senior Lecturer at the Department of Computer Science, Ekiti State University, Ado-Ekiti, Nigeria. She was also the Ag. Head of the Department of Computer Science, Ekiti State University from 2020-2022. She is a member of professional bodies which include the Computer Professional [Registration Council of Nigeria (CPN)] and the Association for Computing Machinery (ACM). Also, a Postdoctoral research fellow at the Department of Computer Science and Information Technology, Sol Plaatje University, Kimberley, South Africa. Her research interests include recommender systems, information systems, and machine learning. She can be contacted at: folasade.isinkaye@eksu.edu.ng.