 http://dx.doi.org/10.14500/aro.11618

Encryption of Color Images with a New Framework: Implementation Using Elzaki Transformation

Mardan A. Pirdawood[1*], Shadman R. Kareem[1,2] and Omar Al-Rassam[1]

[1]Department of Mathematics, Faculty of Science and Health, Koya University, Danielle Mitterrand Boulevard, Koya KOY45, Kurdistan Region – F.R. Iraq

[2]Department of Computer Science, College of Information Technology and Computer Sciences, Catholic University in Erbil, Kurdistan Region – F.R. Iraq

***Abstract*— The significance of image encryption has risen due to the widespread use of images as a key means of sharing data across different applications. Encryption methods are crucial in defending the confidentiality and integrity of valuable image data. This work proposes a novel method of image encryption technique based on the Elzaki transformation and substitution process, which is made possible by the extension of the Maclaurin series coefficients. The image is encrypted using an infinite series of hyperbolic functions and the Elzaki transform; the inverse Elzaki transform is then used to decrypt the image. Using modular arithmetic, the coefficients that result from the transformation are keyed.**

***Index Terms*—Cryptography, Elzaki Transformations, Image Encryptions, Maclaurin Series**.

I. Introduction

The widespread use of image data in various multimedia applications highlights the crucial need to secure such data for communication and storage purposes. In the realm of protecting private information, image encryption emerges as an effective technique, with several methods proposed for communication purposes (Yang and Wang, 2021; Kaur and Jindal, 2019; Sui, Duan and Liang, 2015). Image encryption presents notable differences compared to text encryption, due to several important factors, including the large amount of data that images contain and the intricate correlations between pixel values. This complexity arises from the multidimensional character of images, where each pixel contributes to the overall composition and visual content. Unlike text, which is typically represented as a linear sequence of characters, images contain rich spatial and color information, requiring encryption methods that can effectively preserve these attributes while ensuring security. Thus, image encryption methods must navigate the intricacies of image representation and processing, making them distinct from traditional text-based encryption approaches. Traditional encryption methods such as advanced encryption standard (AES), data encryption standard (DES), and Rivest-Shamir-Adleman (RSA) are considered inappropriate for image encryption due to their higher processing time requirements. In recent work, non-standard encryption techniques have mostly been used to encrypt digital media to improve both speed and security requirements. These unconventional methods employ techniques for changing and rearranging (substitution and permutation). The image encryption algorithm described combines several techniques to enhance security and reduce confusion in the encryption process. Based on the algorithm of complete shuffling and the transformation of a substitution box, this proposed algorithm presents extra confusion (Hamad and Farhan, 2020).

To achieve crucial encryption characteristics, namely, confusion and diffusion, image encryption algorithms manipulate the pixel values of the image. Confusion refers to the complex and nonlinear transformation of pixel values, making it challenging for adversaries to discern any patterns or relationships within the encrypted image. This ensures that even small changes in the input image result in significant alterations in the encrypted output. Derived from the wavelet transform (Wei and Liu, 2023; An and Liu, 2019), chaos theory (Elshamy, et al., 2019; Liu, Sun and Zhu, 2016), and discrete cosine transform (DCT) (Wang, Liu and Jiang, 2021; Liang and Xiao, 2020). These investigations have significantly enriched the literature in the field, showcasing the wide array of approaches adopted to secure digital images. A novel strategy grounded in multi-chaotic theory is put forth. To create an effective encryption that is challenging to crack, the study also employed two distinct dimensions to build S-box. Process using a single keystream generator, shift process (based on 3D Lorenz map) related diffusion operations, and produce S-box (based on 2D Henon map) related confusion operations (Nasry, et al., 2022, August.)

ARO-The Scientific Journal of Koya University
Vol. XII, No. 1 (2024), Article ID: ARO.11618. 11 pages
Doi: 10.14500/aro.11618
Received: 04 October 2023; Accepted: 16 May 2024
Regular research paper: Published: 14 June 2024
Corresponding author's e-mail: mardan.ameen@koyauniversity.org

Amitava Nag, et al. introduced an innovative encryption approach centered on location transformation. Their strategy involved employing the method of the affine transform and utilizing four 8-bit keys for dispersing pixel data across the entire image. Subsequently, the image was divided into 2 × 2-pixel chunks, with each block being encrypted using the XOR algorithm and the four 8-bit keys (Nag, et al., 2011, July; Priya, et al.). Another study introduced a groundbreaking methodology for the encryption and decryption of color images, wherein the researchers presented an innovative solution based on the "SEE transform." The study extensively delved into encryption technology, offering comprehensive insights into the proposed approach (Kuffi, Mehdi and Mansour, 2022, August).

Integrating various cryptographic techniques has become pivotal in enhancing the robustness and versatility of security measures. The amalgamation of multiple methodologies in cryptography aims to address the evolving challenges posed by diverse data types and security requirements (Hamad and Farhan, 2020). Noteworthy among these integrated approaches is the fusion of symmetric and asymmetric encryption algorithms, leveraging the strengths of both for heightened security.

The fusion of various methodologies enables the creation of enhanced security modules that address security concerns and yield more dependable outcomes in image processing. This amalgamation of techniques is exemplified in Al-Khazraji, Abbas and Jamil (2022), wherein they introduced an innovative model amalgamating deep dreaming with neural style transfer (NST). In their research, the authors constructed a model that merges deep dreaming and NST to generate novel images. The utilization of VGG-19 and Inception-v3 pre-trained networks was employed for NST and deep dream, respectively. The study revealed that varying images result in distinct loss values, contingent on the clarity levels inherent in each of those images. Subsequent to this development, numerous alternative methodologies for image encryption have been proposed through the integration of diverse techniques. Manisekaran, the proponent, advocates for the adoption of an innovative methodology wherein enhancements are made to both the key space and the encryption process. The encryption process involves subjecting the DCT of the image to encryption through a generalized logistic equation. This innovative approach facilitates simultaneous compression and encryption. Before the application of the DCT, an Arnold cat map is employed to shuffle the image. The efficacy of the proposed compression and encryption method is substantiated through the examination of various chaotic metrics, including bifurcation diagrams and mutual information (Pradheep, 2021).

The Elzaki transformation, a mathematical technique known for its efficacy in cryptographic applications, was strategically applied to transform the information into a secure format, rendering it less susceptible to unauthorized access. Concurrently, the congruence modulo operator played a pivotal role in preserving the integrity of the encrypted information during the encryption and decryption processes. The researchers employed the Elzaki transformation in conjunction with the congruence modulo operator to ensure the security and subsequent decipherment of a concealed piece of information (Salim and Ashruji, 2016). Furthermore, the Laplace integral transforms and their inverses represent pivotal counterparts within the domain of cryptographic techniques, having a critical impact on the security and functionality of cryptographic processes. Laplace integral transforms application in cryptography and underscores the utilization of advanced mathematical methods to enhance data security (Shivaji and Hiwarekar, 2021), for instance. This study examines the prerequisites for developing an encryption method based on the Laplace transform. In addition, it explores strategies aimed at fortifying the identified vulnerabilities inherent in said cryptographic process. A proposed modification to the initial step of the encryption scheme is presented, resulting in the generation of two distinct passwords for a singular iteration. This modification serves the dual purpose of enhancing the overall security of the encryption process while addressing potential sources of weakness. The amalgamation of diverse techniques yields the capacity to formulate additional security modules within the domain of security. Concurrently, such integration enhances the dependability of outcomes in the context of image processing, particularly concerning security considerations. This multifaceted approach to security not only broadens the repertoire of available protective measures but also ensures a heightened level of reliability in addressing security concerns, specifically in the realm of image processing applications. In Pirdawood, Kareem and Zahir (2023), the researchers articulate a novel encryption methodology tailored for real-time audio applications. The encryption process involves the application of hyperbolic functions and the Laplace transform to secure the audio data. Subsequently, the decryption of the encrypted sound is executed through the inverse Laplace transformation process (Wang et al., 2015). Key generation, crucial for the establishment of a set of coefficients derived from the transformation, is systematically conducted by employing a modular arithmetic rule. The other transformation to encrypt the audio was introduced. Farsana, Devi and Gopakumar (2023) introduce an audio encryption algorithm predicated on the permutation of audio samples, achieved through the utilization of a discrete modified Henon map, followed by a substitution operation employing a key stream generated from the modified Lorenz-hyperchaotic system. The methodology commences with the application of the fast Walsh–Hadamard transform to compress the initial audio file, thereby eliminating residual intelligibility in the transformed domain. Subsequently, the encrypted file undergoes a two-phase encryption process.

In this research, we developed a novel mathematical transformation for cryptography that involves the integration of hyperbolic functions, specifically, the Elzaki transform, for encrypting digital image data and its corresponding inverse Elzaki transforms for decryption purposes. The transformation, defined over a finite field, is recursively applied to blocks of samples extracted from a non-compressed digital image input, with the secret key determining the number of iterations of the transformation

 http://dx.doi.org/10.14500/aro.11618

applied to each block. Confusion is achieved through the manipulation of power series coefficients. The approach that we have chosen has been previously utilized across various disciplines by numerous researchers. For instance, Elzaki (2011) innovatively employed power series transformations in a creative way to encrypt a certain text in cryptography. This was achieved through the utilization of the extended Elzaki transform of an exponential function. The construction of the key involved applying the principles of modular arithmetic to the transformation coefficients. Furthermore, we utilize this technique to encrypt digital picture data by combining the Elzaki transformation, which is applied to the Maclaurin series coefficients, with the Maclaurin series of the cosine hyperbolic transform.

II. The Elzaki Transform

The Elzaki transforms, introduced by Elzaki in 2011, have garnered considerable prominence in both the applied mathematics and engineering domains. This transformative mathematical tool has found widespread utility, demonstrating its efficacy in various applications. Its introduction has significantly influenced the resolution of mathematical problems and engineering challenges.

The application of the Elzaki transforms in digital image processing extends its reach beyond its origins in applied mathematics and engineering. In the realm of digital image processing, the Elzaki transform emerges as a valuable mathematical tool with the potential to contribute to various aspects of image analysis and manipulation. In digital image processing, the Elzaki transform's adaptability and unique characteristics make it an intriguing choice for certain applications; see the reference (Elzaki, 2011). The designated functions within set A are contemplated as follows.

$$A=\left\{f(t):\exists M,k_1,k_2>0,\left|f(t)\right|<Me^{\frac{|t|}{k_j}},\text{if } t\in(-1)^j\times[0,\infty)\right\}$$

For a specific function within the set, M should be a finite value, whereas k_1 and k_2 could be either finite or infinite. The Elzaki transformation can be expressed as follows:

$$E[f(t)]=T(s)=s\int_0^{\infty}f(t)e^{\frac{-t}{s}}dt,\ k_1\le s\le k_2,t\ge 0 \tag{1}$$

The Elzaki transformation exhibits linearity, meaning that it follows the principles of a linear transformation, that is,

$$E\{f_1(t)\}=F_1(s),E\{f_2(t)\}=F_2(s),\ldots,E\{f_n(t)\}=F_n(s),$$

if then

$$E\{c_1f_1(t)+c_2f_2(t)+\ldots+c_nf_n(t)\}=c_1F_1(s)+c_2F_2(s)+\ldots+c_nF_n(s), \tag{2}$$

Where $c_1,c_2,\ldots,c_n$ represent constant values (Elzaki, 2011). Below are the descriptions of the Elzaki transformation and the inverse Elzaki transform for several elementary functions:

- $E(a)=au^2$ where a is constant,
- $E(t^n)=n!s^{n+2}$,
- $E^{-1}(s^2)=1$,
  $E^{-1}(s^{n+2})=t^n/n!$.

III. Proposed Method

The following steps outline the application procedures that enhance data security and privacy in the proposed hybrid mode Elzaki transformation through the integration of cryptography and encryption technology. The encryption of the color image is accomplished through the utilization of the Elzaki transform, while the corresponding inverse Elzaki transform is employed for the decryption process.

A. Encryption

The encryption procedure is delineated into three distinct phases, each integral to the overarching process. These phases include

(i) Key Generation

The initial phase of the encryption process involves the generation of cryptographic keys. These keys play a pivotal role in ensuring the security and confidentiality of the data.

(ii) Color Change

The subsequent phase introduces a transformative step known as color alteration. This facet of the encryption process focuses on modifying the color attributes of the data, contributing to obfuscation, and adding a layer of security to the encrypted information.

(iii) Maclaurin Series Application (t cosh t)

The final phase incorporates the utilization of the Maclaurin series, specifically pertaining to t cosh t. This mathematical series is invoked as a crucial component in the encryption algorithm, contributing to the intricate transformation of the data. The Maclaurin series expansion involving hyperbolic cosine functions is employed to achieve a nuanced and effective encryption strategy.

The Maclaurin series expansion of t cosh t is mathematically expressed as:

$$t\cosh t=\sum_{i=0}^{\infty}\frac{t^{2i+1}}{2i!} \tag{3}$$

It intended for encryption as input to conduct simulation studies. The implementation of this proposed approach was realized through the utilization of MATLAB. In this phase, the dynamic original image undergoes a transformative process, resulting in an encrypted image. Notably, within the Maclaurin series of t cosh t stage, pixel values undergo simultaneous alterations, whereas the color modification is facilitated through the application of the Elzaki transform.

Step 1: Choose the color plain image P (M,N,3), where M×N is the size of the RGB components of the plain image.

Step 2: Make the entries P_{ij} of the matrix P for the RGB components as the coefficients of the Maclaurin series of t

cosh t as follows:

$$\text{Pt}\cosh t = \sum_{j=0}^{\infty} \frac{P_{ij}}{2j!} t^{2j+1}, \text{ where i=1,2,…M and } P_{ij}=0, \text{ for j > N} \quad (4)$$

Step 3: Utilizing the Elzaki transformation for Equation (4), we derive the transformed expression, as follows:

$$E\left[\sum_{j=0}^{\infty} \frac{P_{ij}}{2j!} t^{2j+1}\right] = s\int_0^{\infty}\sum_{j=0}^{\infty} \frac{P_{ij}}{2j!} t^{2j+1} e^{\frac{-t}{s}} dt = \sum_{i=0}^{\infty} P_{ij}(2j+1)s^{2j+3}$$

$$= \sum_{i=0}^{\infty} q_{ij} s^{2j+3} \quad (5)$$

Where $q_{ij}=P_{ij}(2j+1)$, for i=0,1,2,…,N, and j=1,2,…,N.

Step 4: Find C_{ij} such that $q_{ij} \cong C_{ij}$ mod 256, for i=0,1,2,…,N, and j=1,2,…,N, for all of the three RGB-image components. Thus, the RGB-encoded image C become "M×N×3".

Note that, the plain image P(M,N,3) in terms of i and j, for i=0,1,2,…M and j=1,2,…,N under the Elzaki transform of Pt cosh t can be converted to cipher image C, where the components of this matrix are given by

$$C_{ij} = q_{ij} - 256K_{ij} \quad (6)$$

and

$$q_{ij} = (2j+1)P_{ij} \quad (7)$$

with key

$$K_{ij} = \frac{q_{ij} - C_{ij}}{256} \quad (8)$$

Consequently, the key matrix will assume dimensions of K(M,N,3). To illustrate, Fig. 1 presents a visual representation of the key within the histogram diagram during the RGB encryption process applied to the Lena image.

A. Decryption Algorithm

The decryption process serves as the inverse operation to encryption. During decryption, the input is the RGB-encrypted image represented as a Vector C, as depicted in Fig. 2 for illustrative purposes. The secret key, denoted as K(M,N,3) in accordance with Equation (8), is employed in this process, ultimately resulting in the generation of the decrypted image. The ensuing decryption procedure encompasses a series of sequential steps aimed at reconstructing the original image from its encrypted form.

Step 1: Choose the RGB-encrypted image C(M,N,3), where M×N is the size of the RGB components of the RGB-encrypted image.

Step 2: Find q_{ij} such that $q_{ij} \cong C_{ij}$ mod 256 for i=0,1,2,…,M and j=1,2,…,N, for all of the three components of the RGB-image. Then, make it as the coefficient of the follow series:

$$T(s) = \sum_{i=0}^{\infty} q_{ij} s^{2j+3} \quad (9)$$

Step 3: Utilizing the Elzaki inverse transformation for Equation (9), we derive the transformed expression, as follows:

$$E^{-1}\left[\sum_{i=0}^{\infty} q_{ij} s^{2j+3}\right] = E^{-1}\left[\sum_{i=0}^{\infty} P_{ij}(2j+1)s^{2j+3}\right] = \sum_{j=0}^{\infty} \frac{P_{ij}}{2j!} t^{2j+1}$$

$$= \text{Pt}\cosh t \quad (10)$$

where $P_{ij} = \frac{q_{ij}}{(2j+1)}$, for i=0,1,2,…,M and j=1,2,…,N

Step 4: The matrix P(M,N,3) become the RGB-decrypted image.

IV. Results and Simulation Analysis

A comprehensive assessment was conducted on a multitude of color images, and the outcomes demonstrated uniform consistency. Specifically, images featuring Lena, Baboon, and Sailboat on Lake, sourced from the USC-SIPI image database (Weber, 2006), as well as Lya, were considered as original experimental photographs for simulation purposes. The proposed RGB photo encryption technique incorporates the application of the Elzaki transformation, employing the following key components:

- Red component only (R-Encryption),
- Green component only (G-Encryption),
- Blue component only (B-Encryption),
- The concurrent integration of both elements is associated with the red and green components (RG-Encryption),
- The concurrent integration of both elements is associated with the red and blue components (RB-Encryption),
- The concurrent integration of both elements is associated with the green and blue components (GB-Encryption),
- All the red, green, and blue components together (RGB-Encryption).

As depicted in Fig. 1, our experimental results based on

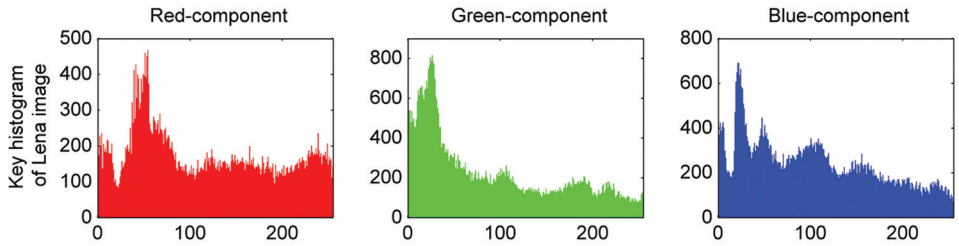

Fig. 1. The histogram embodies the key matrix *K* (*M*, *N*, 3) for the Lena image.

http://dx.doi.org/10.14500/aro.11618

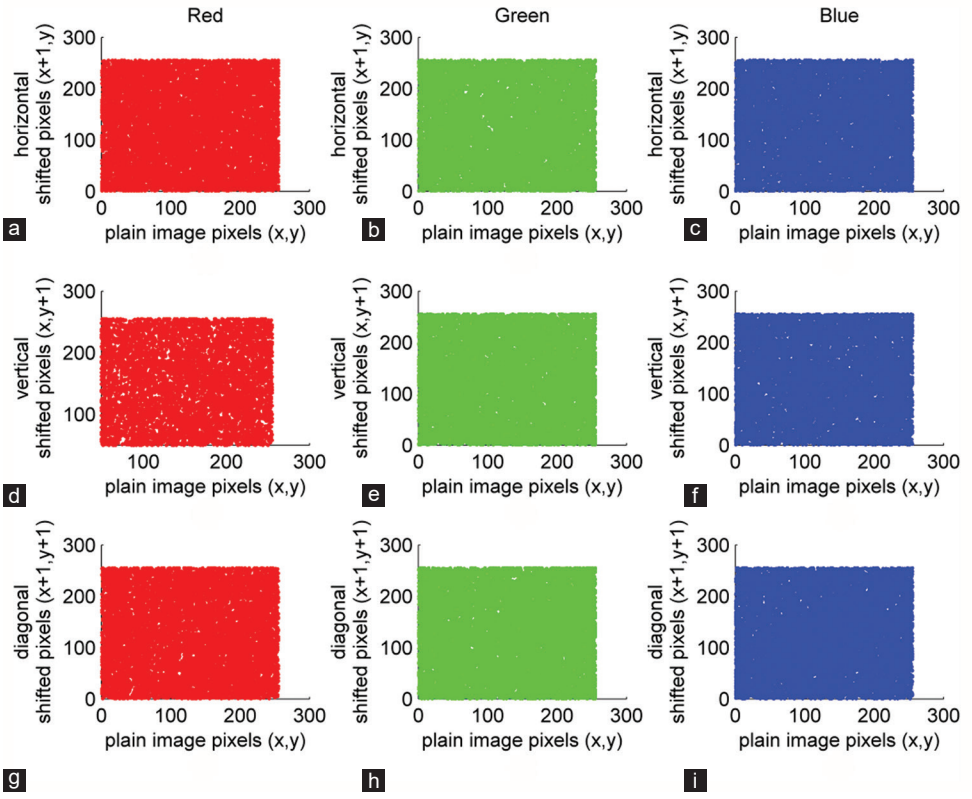

Fig. 2. Correlation analysis was conducted on the RGB-encrypted image of Lena, involving the examination of horizontally, vertically, and diagonally correlated pixels. The analysis specifically centered on three components of the RGB-encrypted image, denoted as the red, green, and blue components (a, d, g), (b, e, h), and (c, f, i), respectively.

the proposed approach are showcased using the reference image, denoted as "Lena 256 × 256 × 3," serves as the unaltered basis and is visually represented in Fig. 3 in the RGB format. The proposed methodology is to be executed using MATLAB R2016a. The implementation transpired on an individual computing system, featuring an Intel(R) Core(TM) i5-1135G7 central processing unit operating at a clock speed of 2.42 GHz. The computational unit is equipped with a capacious 1 TB hard disk drive for storage and a substantial 8 GB of RAM to facilitate efficient memory operations. The operating environment for this implementation was Windows 11 Pro.

A. Statistical Analysis

Numerous statistical evaluations on the generated procedures are carried out to assess the dependability of the suggested encryption cryptosystem. To determine the efficacy and resilience of the encryption technique, we offer comprehensive insights into the findings of these investigations in this part. In addition, the statistical studies explore the analysis of encryption outputs, including pixel value distributions, correlation coefficients, and error metrics like peak signal-to-noise ratio (PSNR) and mean squared error (MSE). These evaluations give important insights into the integrity and dependability of the encrypted data, as well as useful details on how to maintain image security and quality throughout the encryption and decryption procedures.

Histogram analysis

The representation of pixel intensity levels within an image is effectively captured by a histogram, a significant metric that could be exploited by malicious entities to devise potential attacks, particularly if they possess knowledge about pixel frequency patterns across different intensity levels. In the context of encrypted images, it becomes imperative to guarantee that the histograms of these images do not reveal any information derived from the statistical analysis of the original image pixels. The scrutiny of histogram distribution is exemplified in Fig. 3. Specifically, Fig. 3 presents the histograms corresponding to the red, green, and blue components of the unencrypted Lena image, respectively. This examination underscores the importance of mitigating any potential leakage of information through the careful handling of histograms during the encryption process.

The histograms corresponding to the encrypted portions of the image are illustrated in Fig. 3. It is evident that the encrypted image histograms do not reveal any insights into the distribution of intensity levels found in the original image. Nonetheless, prior research underscores that the histogram derived from the fractional domain tends to be constrained to a narrow range of pixel values due to the concentration of transform energy at the center. To mitigate this concern and guarantee a more equitable distribution of energy within the cryptographic framework, achieving a flat or uniform histogram becomes of paramount importance. As depicted in Fig. 3, the histograms of the encrypted image demonstrate a

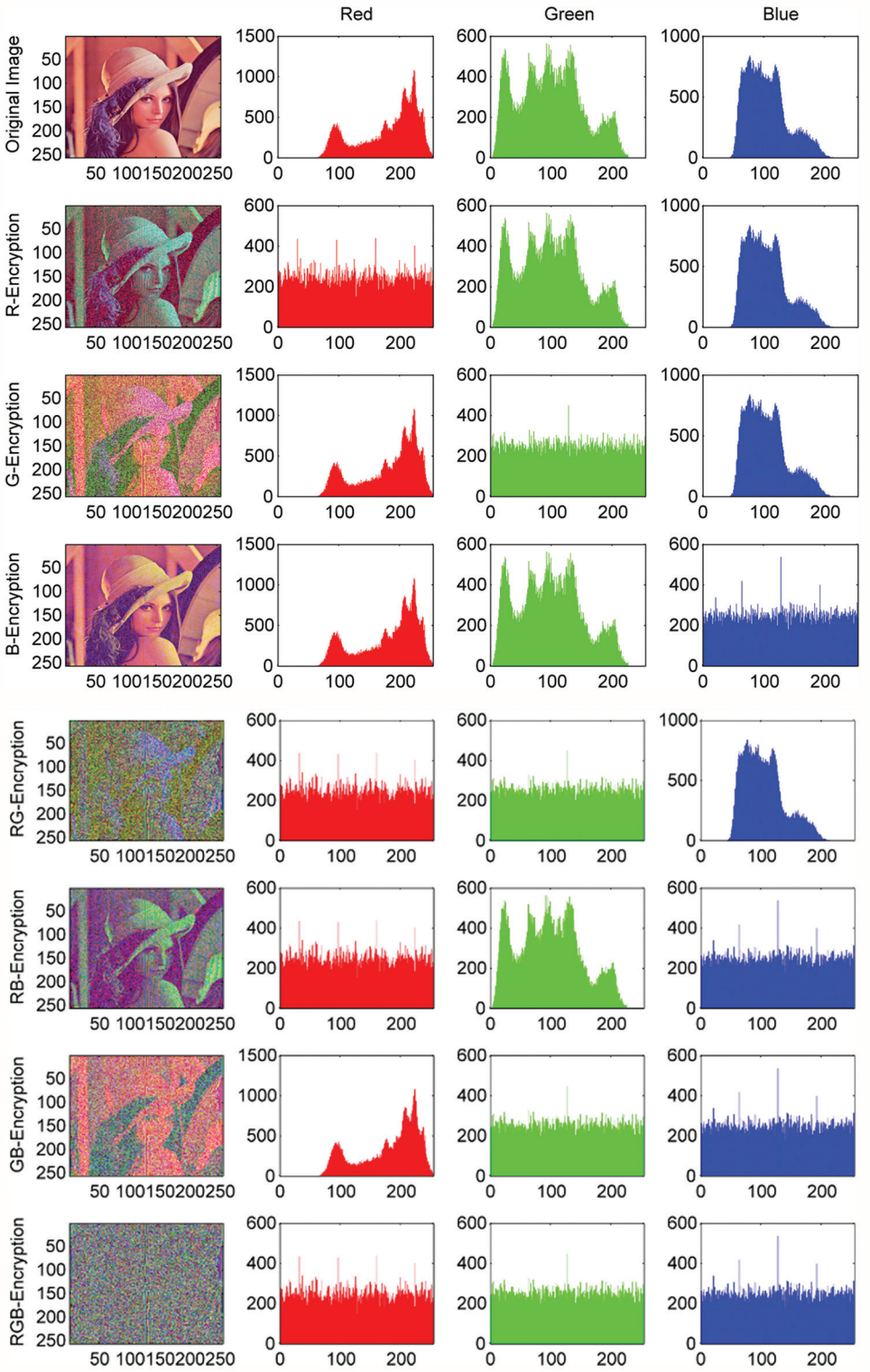

Fig. 3. The observed distribution of correlations distinctly underscores a noteworthy separation among pixel values in the encrypted image, emphasizing the successful accomplishment of decorrelation.

markedly flatter and more uniform pattern when juxtaposed with methodologies documented in recent studies. This observation emphasizes the effectiveness of the proposed approach in attaining a desirable histogram characteristic, contributing to enhanced security in the cryptographic context (Kang, et al., 2017, September; Lang, 2012; Sui, Duan and Liang, 2015; Wu, et al., 2014).

Correlation coefficient analysis

An effective encryption method should have the ability to disrupt the connection between neighboring pixels. The relationship between adjacent pixels in an encrypted image should be minimized. Thus, ensuring the uniform distribution of pixel values across the entire intensity spectrum in both dimensions becomes a crucial factor

http://dx.doi.org/10.14500/aro.11618

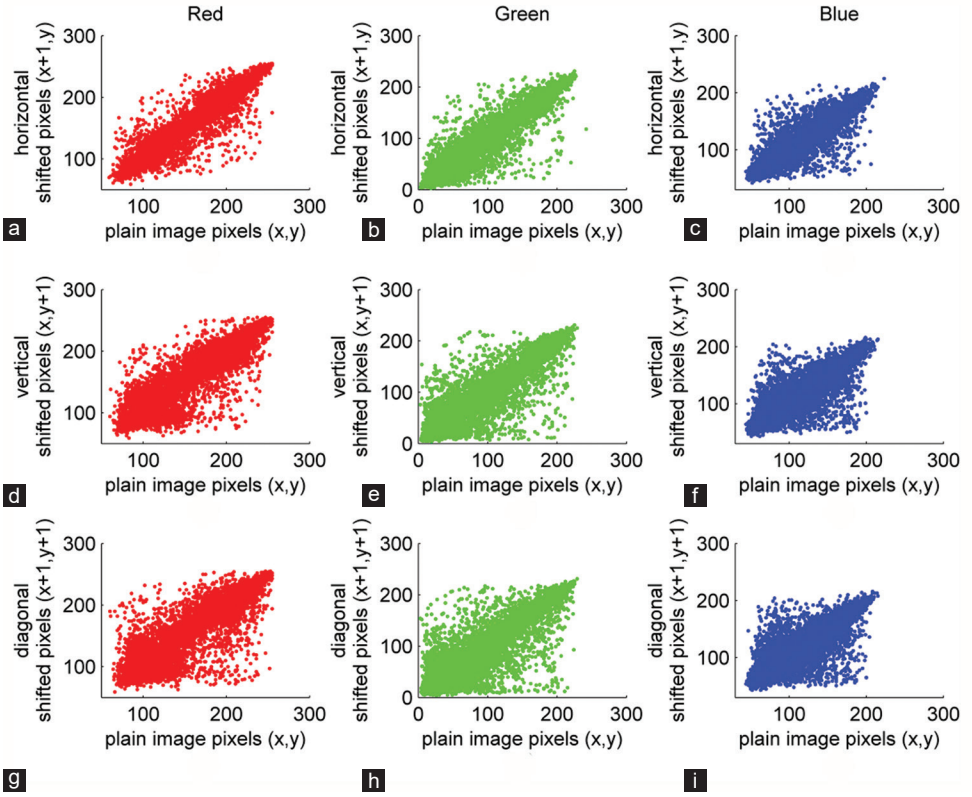

Fig. 4. Correlation analysis was performed on the Lena image, investigating the horizontal, vertical, and diagonal correlations among pixels. The analysis specifically concentrated on the three components of the RGB-original image: The red, green, and blue components denoted as (a, d, g), (b, e, h), and (c, f, i), respectively.

for encrypted image integrity. The distributions of these values have been visually represented in Fig. 4, using the Lena image as an illustrative example. Our analysis predominantly focuses on the individual components of red, green, and blue, delving into the pixel distributions of neighboring elements. The initial column of Fig. 4 showcases the distributions of diagonally, vertically, and horizontally adjacent pixels within the unencrypted source image. In the subsequent column, we present the corresponding correlation patterns for the encrypted image, followed by a third column depicting the same for the decrypted version.

The observed distribution of correlations distinctly underscores a noteworthy separation among pixel values in the encrypted image, emphasizing the successful accomplishment of decorrelation. For a more quantitative evaluation, we calculated correlation coefficients for diverse test images, and the specific outcomes are detailed in Table I.

The calculation of the correlation coefficient will be performed as follow:

$$\rho(x,y)=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left((x_i-\bar{x})(y_i-\bar{y})\right),$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2,\ D(y)=\frac{1}{N}\sum_{i=1}^{N}(y_i-\bar{y})^2,$$

$$\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i,\ \bar{y}=\frac{1}{N}\sum_{i=1}^{N}y_i$$

TABLE I
THE COMPUTATION OF CORRELATION COEFFICIENTS WAS UNDERTAKEN TO SCRUTINIZE THE RELATIONSHIPS BETWEEN ADJACENT PIXELS WITHIN DIFFERENT UNENCRYPTED IMAGES. THIS COMPREHENSIVE ANALYSIS EXTENDED TO VERTICALLY, HORIZONTALLY, AND DIAGONALLY ADJACENT PIXEL PAIRS. FURTHERMORE, THE IDENTICAL CORRELATION COEFFICIENTS WERE CALCULATED FOR THEIR CORRESPONDING RGB-ENCRYPTED IMAGES

Images	Direction	Plain-image correlation coefficients			RGB-encrypted-image correlation coefficients		
		Red	Green	Blue	Red	Green	Blue
Lena	Horizontal	0.9704	0.9553	0.9126	0.1026	0.0616	0.0482
	Vertical	0.9448	0.9204	0.8746	−0.0145	−0.0102	−0.0029
	Diagonal	0.9218	0.8994	0.8548	−0.0219	0.0056	−0.0093
Baboon	Horizontal	0.8183	0.6609	0.8075	0.0338	0.0128	0.0127
	Vertical	0.8626	0.7251	0.8162	8.8268e-4	−0.0040	−0.0085
	Diagonal	0.8090	0.6430	0.7772	−7.5326e-5	−0.0028	−0.0088
Sailboat on Lake	Horizontal	0.9201	0.9272	0.9401	0.0390	0.0546	0.0832
	Vertical	0.9234	0.9354	0.9377	−0.0069	0.0010	−0.0259
	Diagonal	0.8886	0.8943	0.9099	−0.0148	−0.0132	−0.0258
Lya	Horizontal	0.9813	0.9449	0.9295	0.1093	0.1013	0.0976
	Vertical	0.9799	0.9423	0.9259	−0.0123	0.0032	−0.0195
	Diagonal	0.9742	0.9279	0.9078	−0.0141	0.0017	−0.0171

The range of ρ(x,y) values spans from −1 to 1. A value of ρ(x,y)≈1 denotes a robust correlation between adjacent pixels, while of ρ(x,y)≈0 suggests no correlation. Negative values indicate an inversion in one of the series. Table I provides the correlation coefficients for both plain and encrypted image. To demonstrate the efficacy of the proposed approach with respect to correlation coefficients, a comparative evaluation is presented in Table I, employing the Lena image as a reference point.

The secret key $K(M_0,N_0,3)$ is derived during the RGB-encryption process for the Lena image, as illustrated in Fig. 1.

To enhance our comprehension and gain further insights into this technique, we have the opportunity to conduct additional experiments on various other images, as shown in Fig. 5. By exploring its performance on different types of images, we can deepen our understanding of how this technique functions across diverse scenarios.

In comparing the proposed method with the results presented in Table II, it's important to note that correlation coefficients measure the linear relationship between two variables. Our scheme generally demonstrates commendable correlation coefficients with the original Lena image and its encrypted versions image across the horizontally, vertically, and diagonally correlated pixels. However, a notable discrepancy arises in the vertical direction. Furthermore, an intriguing aspect pertains to the divergent behavior of distinct color channels within our scheme. Variability in correlation preservation among these channels warrants further investigation into underlying mechanisms. While our proposed scheme generally upholds competitive standing in comparison to its counterparts, nuances in correlation outcomes across different spatial orientations and color domains underscore the need for comprehensive analysis and potential refinement. Tackling these intricacies is expected to improve our method's effectiveness and applicability.

Table III presents the correlation coefficients comparing unencrypted images with their encrypted counterparts across various color images. The findings reveal exceedingly low correlation coefficients, approximately approaching zero, indicative of a lack of correlation between the encrypted and unencrypted images. Moreover, the correlation coefficient consistently registers as "1" between the original and decrypted images, providing conclusive evidence of their identical nature. The algorithm's performance was systematically evaluated using diverse images, including Lena, Baboon, Sailboat on Lake, and Lya, thereby affirming its efficacy across a spectrum of image types.

B. Perceptual Security

This section delves into the visual comparison between encrypted data and the original plain image. Two distinct

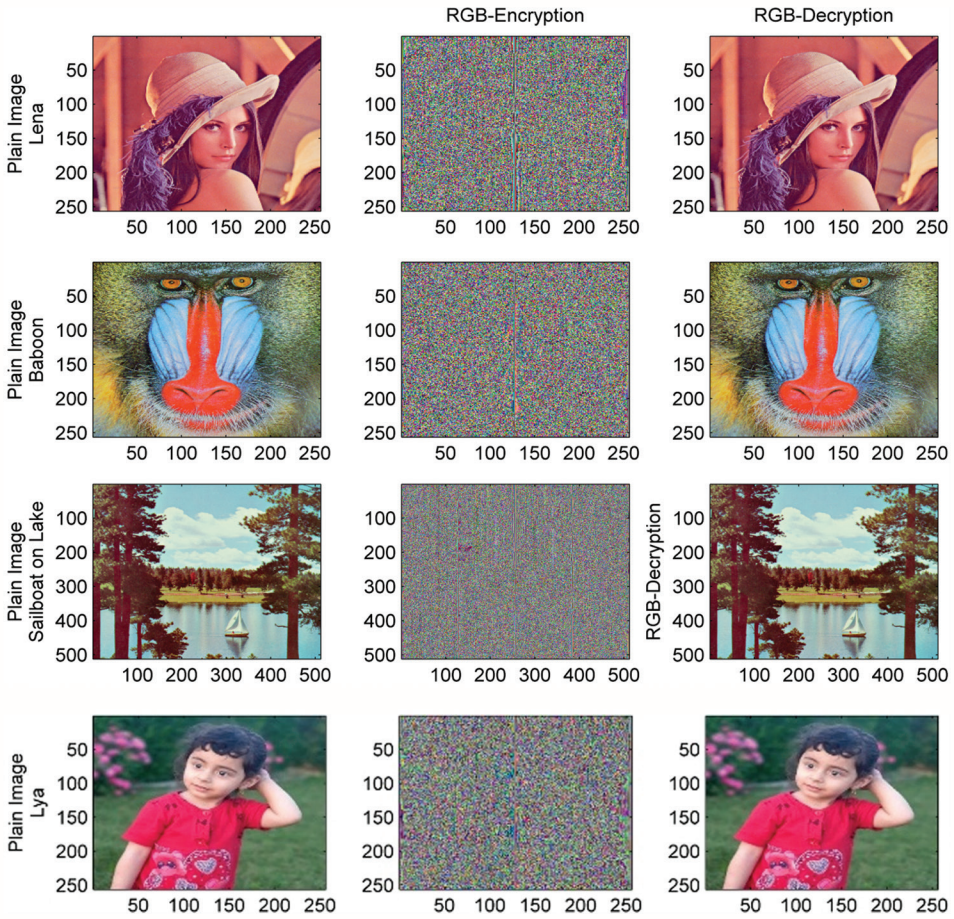

Fig. 5. Plain, RGB-encrypted, and RGB-decrypted images of Lena, Baboon, and Sailboat on Lake and Lya.

examinations are undertaken to assess the extent to which the proposed encryption method preserves visual quality. These evaluations encompass both subjective and objective analyses, collectively offering a comprehensive assessment of the visual security of the encryption process (Lian, 2008).

Visual evaluation

Fig. 3 provides a comprehensive visual representation of our analysis. The original RGB color presentation of Lena is exhibited in Fig. 3. We systematically explored various potential encryption methods for the RGB components of the Lena image, considering combinations such as {ϕ, R, G, B, RG, RB, GB, RGB}, with ϕ representing exclusion. Among the seven conceivable combinations, the RGB-encryption method yielded the most favorable outcomes, as illustrated in Fig. 3.

This preference is grounded in the efficacy of RGB-encryption, which effectively eradicates any visually identifiable connections to the original Lena image. This underscores the robust transformative capability inherent in our encryption technique.

Assessing perceptual quality through objective measures

An alternative method of assessment entails the scrutiny of impartial criteria employed to assess excellence, as illustrated in Table IV. The subsequent section provides a mathematical elucidation of these specific measures of inaccuracies. Readers are encouraged to delve into the details presented in Table IV to acquire a comprehensive understanding of the outcomes.

TABLE II
Analysis of Correlation Coefficients in Comparison (Lena Image)

Lena image	The encrypted image's correlation coefficients		
	Horizontal	Vertical	Diagonal
Zhou, et al. (2014)	0.0864	0.0583	0.0931
Pan, et al. (2016)	0.0249	0.0505	0.0280
Kaur and Jindal (2019)	0.5051	0.0020	−0.0010
Faragallah, et al. (2019)	−6.6700e-5	0.0367	0.0247
Proposed scheme			
Red	0.1026	-0.0145	−0.0219
Green	0.0616	-0.0102	0.0056
Blue	0.0482	-0.0029	−0.0093

1) MSE: An alternative approach to assess the dissimilarity between visually distinct images involves the utilization of the mean square error (MSE). This metric will be applied to compute disparities between images, where a higher MSE value signifies greater dissimilarity between the compared images. Ideally, in the context of comparing two highly similar images, the MSE should yield a value approaching zero.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(P_{ij} - C_{ij}\right)^2}{M \times N} \tag{12}$$

In the equation, P_{ij} and C_{ij} denote the pixel values situated at the (i,j) coordinates within the plain and decoded images, respectively. The dimensions of the image are determined by the product of M and N. When conducting comparisons between encrypted photographs and their corresponding original images, the MSE results presented in Table IV reveal significant values, approximately around 10,000. These values indicate a discernible visual distinction between the two sets of images.

2) PSNR measurement: The PSNR quantifies spectral information and mirrors the likeness between a pair of images. Elevated PSNR values suggest greater The PSNR serves as a quantitative measure of spectral information and reflects the resemblance between a pair of images. Higher PSNR values indicate a greater similarity, with this parameter approaching infinity when dealing with two entirely identical pictures. In practical terms, an image is deemed visually meaningful when the PSNR ≥28. The subsequent expression represents its mathematical representation:

$$PSNR = 10 \times \log_{10}\left(\frac{\left(L-1\right)^2}{MSE}\right) \tag{13}$$

For an *n* -bit image, where, *L* typically equals 2^n, representing the maximum pixel intensity value, the average squared difference between the plain and encrypted images is quantified by the MSE. Given the notably low PSNR values ((<< 28) observed in the encoded image, it can be inferred

TABLE III
Correlation Coefficients for Certain Images

Images	Size	Component	Evaluating the correlation coefficients between original and RGB-encrypted images.	Evaluating the correlation coefficients between original and RGB-decrypted images.
Lena		Red	−0.0049	1
	256×256	Green	−5.0293e-4	1
		Blue	−0.0026	1
Baboon		Red	5.4068e-4	1
	256×256	Green	−0.0042	1
		Blue	−0.0079	1
Sailboat on Lake		Red	0.0013	1
	256×256	Green	0.0202	1
		Blue	0.0098	1
Lya		Red	−0.0217	1
	256×256	Green	0.0042	1
		Blue	−0.0044	1

TABLE IV
QUANTITATIVE MEASURES EVALUATING THE PERCEPTUAL EXCELLENCE OF THE PLAIN IMAGE COMPARED TO THE ENCRYPTED IMAGE AND DECRYPTED IMAGE

Images	Size	Component	Original plain image with encrypted image		Original plain image with decrypted image.	
			MSE	*PSNR*	*MSE*	*PSNR*
Lena	256×256	Red	1.0627e+4	7.8668	0	∝
		Green	8.9963e+3	8.5902	0	∝
		Blue	7.0973e+3	9.6199	0	∝
Baboon	256×256	Red	8.5137e+3	8.8296	0	∝
		Green	7.6851e+3	9.2743	0	∝
		Blue	9.4692e+3	8.3677	0	∝
Sailboat on Lake	256×256	Red	7.2657e+3	9.5180	0	∝
		Green	1.1333e+4	7.5875	0	∝
		Blue	1.1449e+4	7.5430	0	∝
Lya	256×256	Red	1.1513e+4	7.5188	0	∝
		Green	8.2606e+3	8.9607	0	∝
		Blue	7.6799e+3	9.2773	0	∝

TABLE V
RGB-ENCRYPTION/DECRYPTION TIME

Image	Size	Extension	RGB-Encryption and Decryption time (S)
Lena	256×256	PNG	0.5174
Baboon	256×256	PNG	0.4293
Sailboat on Lake	256×256	TIFF	0.5095
Lya	256×256	JPEG	0.3746

that these images fail to convey any meaningful details from the original image.

In the comparison of encrypted photographs with their corresponding original images, the PSNR results in Table IV reveal significant values ((<< 28), indicating the absence of additional context in the encrypted photos concerning the plain image. Furthermore, the mean square error between the decrypted and plain images consistently registers as zero across all tested images, as evidenced in Table IV. This outcome underscores the absence of errors resulting from the application of our technique. Consequently, the decrypted counterparts align perfectly with the original images, preserving every single data detail intact.

C. Execution Time

Time emerges as a pivotal consideration when formulating an encryption strategy. The efficacy of an encryption algorithm in maintaining its security level is maximized when its execution time is minimized. The proposed method, leveraging the Elzaki transformation for color image encryption and decryption, guarantees a harmonious balance between speed and security. Comprehensive findings pertaining to the duration of the color images utilized in the encryption and decryption processes are elucidated in Table V.

V. CONCLUSION

In the present study, a framework for encryption ensures the security of color image applications. The design framework encrypts the color image to safeguard confidentiality. The proposed work suggests a novel cryptographic technique for the encryption of digital images by combining an infinity series of specific hyperbolic functions with Elzaki transforms for encryption and corresponding inverse Elzaki transforms for decryption. The private key in this technique is the sum of multiples of the mod. This makes it extremely difficult for an eyedropper to use a brute-force attack or any other kind of attack to discover the secret key. The process's performance and recorded results unequivocally show that our approach was effective in accomplishing its main goal of sound data encryption. In-depth statistical analyses, comprising evaluations of histograms and correlation coefficients, in addition to metrics such as MSE and PSNR, were utilized to determine how effective the suggested security measure was. The process's execution time was also carefully tracked.

REFERENCES

Al-Khazraji, L.R., Abbas, A.R., and Jamil, A.S., 2022. Employing neural style transfer for generating deep dream images. *Aro-The Scientific Journal of Koya University*, 10(2), pp.134-141.

An, F.P., and Liu, J.E., 2019. Image encryption algorithm based on adaptive wavelet chaos. *Journal of Sensors*, 2019, pp.1-12.

Elshamy, A., Hussein, A., Hamed, H.F.A., Abdelghany, M.A., and Kelash, H.M., 2019. Color image encryption technique based on chaos. *Procedia Computer Science*, 163, p.49-53.

Elzaki, T., 2011. The new integral transform "Elzaki transform". *Global Journal of Pure and Applied Mathematics*, 7(1), pp.57-64.

Faragallah, O.S., Alzain, M.A., El-Sayed, H.S., Al-Amri, J.F., El-Shafai, W., Afifi, A., Naeem, E.A., and Soh, B., 2018. Block-based optical color image encryption based on double random phase encoding. *IEEE Access*, 7, pp.4184-4194.

Farsana, F.J., Devi, V.R., and Gopakumar, K., 2023. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. *Applied Computing and Informatics*, 19, pp.239-264.

Hamad, A.S., and Farhan, A.K., 2020. Image encryption algorithm based on substitution principle and shuffling scheme. *Journal of Engineering Technology*, 38(3B), pp.98-103.

Kang, X., Han, Z., Yu, A., and Duan, P., 2017. Double Random Scrambling Encoding in the RPMPFrHT Domain. In: *2017 IEEE International Conference on Image Processing* (*ICIP*), pp.4362-4366.

Kaur, J., and Jindal, N., 2019. A secure image encryption algorithm based on fractional transforms and scrambling in combination with multimodal biometric keys. *Multimedia Tools and Applications*, 78, pp.11585-11606.

Kuffi, E.A., Mehdi, S.A., and Mansour, E.A., 2022. Color image encryption based on new integral transform SEE. *Journal of Physics: Conference Series*, 2322(1), p.012016.

Lang, J., 2012. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. *Optics and Lasers in Engineering*, 50(7), pp.929-937.

Lian, S., 2008. *Multimedia Content Encryption: Techniques and Applications*. CRC Press, United States.

Liang, Y.R., and Xiao, Z.Y., 2020. Image encryption algorithm based on compressive sensing and fractional DCT via polynomial interpolation. *International Journal of Automation and Computing*, 17(2), pp.292-304.

Liu, W., Sun, K., and Zhu, C., 2016. A fast image encryption algorithm based

on chaotic map. *Optics and Lasers in Engineering*, 84, p.26-36.

Nag, A., Singh, J.P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D., and Sarkar, P.P., 2011. Image Encryption using Affine Transform and XOR Operation. In: *International Conference on Signal Processing, Communication*, *Computing and Networking Technologies*.

Nasry, H., Abdallah, A.A., Farhan, A.K., Ahmed, H.E., and El Sobky, W.I., 2022. Multi chaotic system to generate novel S-box for image encryption. *Journal of Physics: Conference Series*, 2304(1), p. 012007.

Pan, S.M., Wen, R.H., Zhou, Z.H., and Zhou, N.R., 2017. Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform. *Multimedia Tools and Applications*, 76, pp.2933-2953.

Pirdawood, M.A., Kareem, S.R., and Zahir, D.C., 2023. Audio encryption framework using the laplace transformation. *Aro-the Scientific Journal of Koya University*, 11(2), pp.31-37.

Pradheep, M., 2021. *Image Encryption by Using ACGLML*. Munich, GRIN Verlag, p.130.

Priya, S.S.S., KarthigaiKumar, P., Mangai, N.S., and Vanathi, P.T., 2012. Survey on efficient, Low-Power, AES image encryption and bio-cryptography schemes. *SmartCR*, 2, pp.379-390.

Salim, S.J., and Ashruji, M.G., 2016. Application of El-Zaki transform in cryptography. *International Journal of Modern Sciences and Engineering Technology*, 3, pp.46-48.

Shivaji, J.S., and Hiwarekar, A.P., 2021. Cryptographic method based on Laplace-Elzaki transform. *Journal of the Maharaja Sayajirao University of Baroda*, 55(1), pp.187-191.

Sui, L., Duan, K., and Liang, J., 2015. Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. *Optics Communications*, 343, pp.140-149.

Wang, X., Liu, C., and Jiang, D., 2021. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Information Sciences*, 574, p.505-527.

Wang, Z.Y., Zhang, Y.Q., and Bao, X.M., 2015. A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering*, 73, p.53-61.

Weber, A.G., 2006. The USC-SIPI Image Database: Version 5. Available from: http://sipi.usc.edu/database [Last accessed on 2023 Oct 01].

Wei, L., and Shi, H., 2023. Chaotic image encryption algorithm based on wavelet transform. *Journal of Applied Mathematics and Computation*, 7(3), pp.359-364.

Wu, J., Guo, F., Liang, Y., and Zhou, N., 2014. Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform. *Optik*, 125(16), pp.4474-4479.

Yang, J., and Wang, X., 2021. A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient. *Information Sciences*, 569, p.217-240.

Zhou, N., Zhang, A., Zheng, F., and Gong, L., 2014. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics and Laser Technology*, 62, pp.152-160.