IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 October 2022, accepted 30 January 2023, date of publication 3 February 2023, date of current version 8 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3242311

RESEARCH ARTICLE

Color Image Encryption Through Chaos and KAA Map

WASSIM ALEXAN[1], (Senior Member, IEEE), MARWA ELKANDOZ[2], MAGGIE MASHALY[3], (Senior Member, IEEE), EMAN AZAB[4], (Senior Member, IEEE), AND AMR ABOSHOUSHA[2,5]

[1]Communications Department, Faculty of IET, German University in Cairo (GUC), New Cairo 11835, Egypt
[2]Physics Department, Faculty of Basic Sciences, German University in Cairo (GUC), New Cairo 11835, Egypt
[3]Networks Department, Faculty of IET, German University in Cairo (GUC), New Cairo 11835, Egypt
[4]Electronics Department, Faculty of IET, German University in Cairo (GUC), New Cairo 11835, Egypt
[5]Physics Department, Science Faculty, Cairo University, Giza 12613, Egypt

Corresponding author: Wassim Alexan (wassim.alexan@ieee.org)

ABSTRACT The unprecedented growth in production and exchange of multimedia over unsecured channels is overwhelming mathematicians, scientists and engineers to realize secure and efficient cryptographic algorithms. In this paper, a color image encryption algorithm combining the KAA map with multiple chaotic maps is proposed. The proposed algorithm makes full use of Shannon's ideas of security, such that image encryption is carried out through bit confusion and diffusion. Confusion is carried out through employing 2 encryption keys. The first key is generated from the 2D Logistic Sine map and a Linear Congruential Generator, while the second key is generated from the Tent map and the Bernoulli map. Diffusion is attained through the use of the KAA map. An elaborate mathematical analysis is carried out to showcase the robustness and efficiency of the proposed algorithm, as well as its resistance to visual, statistical, differential and brute-force attacks. Moreover, the proposed image encryption algorithm is also shown to successfully pass all the tests of the NIST SP 800 suite.

INDEX TERMS Chaos theory, image encryption, KAA map.

I. INTRODUCTION

An impressive technological revolution materialized in recent decades reshaping human lives. This is easily seen in the advancements in computing, wireless smart devices, the Internet as well as their interconnectivity through heterogeneous 5G networks. Such advancements came hand in hand with expansive developments in multimedia, where huge numbers of files are being exchanged every second around the globe. This has posed security challenges to scientists, mathematicians and engineers, who are now constantly developing new algorithms to secure the transmission of data between any two communication entities. For some time, a number of algorithms were mostly utilized to provide this much needed security. Those included the Data Encryption Standard (DES) and its variant, triple DES (3DES), as well as the Advanced Encryption Standard (AES). While they did provide security for a while, they are no longer suitable for the purposes of image encryption. This is because they have either been proven susceptible to cryptanalysis or are simply not efficient algorithms for image encryption. Unlike textual data, images possess a number of properties that require different encryption algorithms. For example, high-definition (HD) images have very high data payloads. Moreover, adjacent pixels in an image exhibit a very high redundancy and correlation [2].

A review of the literature on image encryption confirms Shannon's theory, where a high level of image security can only be attained through the application of two mutually independent encryption stages, namely, confusion and diffusion [5]. A confusion stage forces every bit in an encrypted image to depend on many parts of the key, thus hiding the connection between the two [32]. While a diffusion stage introduces an avalanche effect, such that a change of a single bit in the plain image would result in a change of roughly

The associate editor coordinating the review of this manuscript and approving it for publication was Gangyi Jiang.

half of all the bits in the encrypted image. The purpose of diffusion is to eliminate any statistical relationship from being exhibited between a plain image and its corresponding encrypted one [35]. It is in the design of those two stages of encryption where chaotic functions come into play. Chaotic functions exhibit a number of inherent characteristics that make their use advantageous in relation to communication security. Those characteristics include sensitivity to initial conditions, ergodicity, pseudo-randomness, control parameters and periodicity, to name a few [24]. In general, chaotic functions are classified either into one-dimensional (1D) or multi-dimensional (MD). The choice of adopting 1D over MD chaotic functions for their utilization in image encryption algorithms is always a matter of trade-off between complexity and security. One-dimensional chaotic functions provide simple software and hardware implementations at the price of acceptable security. This makes them ideal for image encryption applications requiring real-time efficiencies. On the other hand, MD chaotic functions provide excellent security but do achieve at the price of more complex designs and implementations [7].

The utilization of multi-dimensional chaotic maps for the purposes of image encryption is very well documented in the literature. For example, the Lorenz system of differential equations is employed in [3], [18], and [51]. The authors of [3] use the Lorenz system as the first encryption stage in a 3-stage encryption process. The other 2 stages involve an S-box and Rule 30 cellular automaton. The authors of [18] apply different scan patterns to each of the RGB color channels of the image to be encrypted. Next, they separate the Lorenz equations and apply the use of each equation on a different color channel. In [51], the Lorenz system is modified, by adding a delay coupling and a mod function, and employed in a single-stage image encryption algorithm. Other MD chaotic functions are also found in the literature. An interesting work is proposed in [6], where the authors utilize a modified Chua's circuit, which exhibits a hyper-chaotic behavior, as a pseudo-random number generator (PRNG) for encryption. In their proposed algorithm, SHA-256 is employed to generate the initial set of secret keys. The authors of [34] make use of a 2D Logistic-adjusted-Sine map to carry out confusion of the RGB pixels, while a single neuron model is employed to generate the key. Their proposed diffusion process is based on a hash value of the plain image. In [15], the authors propose a 3-stage algorithm that incorporates the use of a Chen hyperchaotic function, in addition to an S-box and various fractals. The Julia fractal set is utilized to generate the keys, while the Hilbert fractal is utilized to construct the S-box.

Many works in the literature showcase algorithms that combine the use of more than a single 1D or MD chaotic functions to achieve high levels of image encryption. The authors of [11] combine the use of the Logistic system with the hyperchaotic Chen system, in addition to a dynamic zigzag pattern which depends on the dimensions of the plain image being encrypted. The idea of utilizing a dynamic key is also proposed by the authors of [1] who combine the use of a fractional order chaotic map with elliptic curves. In [40], the authors employ a composite chaotic map, a staged Logistic map, as well as a Tent map to generate their primary encryption key. Then, an Arnold map is utilized to carry out an image scrambling process. The authors of [23] present an image encryption algorithm with a diffusion step that is based on a Lorenz-Rossler chaotic system, while their confusion step is based on 2D Logistic maps. In [13], an efficient algorithm based on hyper-chaos and a vector operation is proposed. The author of [13] employs a post-processing technique to a create a key matrix which reduces the required number of iterations needed for the hyperchaotic system. The authors of [4], propose a 3-stage image encryption algorithm that makes use of a piece-wise linear chaotic map (PWLCM), a chaotic-map-based S-box and the logistic map. The strength of their algorithm emanates from the large positive Lyapunov exponent of the utilized PWLCM. In [16], the authors propose a cloud model Fibonacci dynamical system. Their proposed system builds upon combining a cloud model with a Fibonacci sequence and a quantum Logistic 3D map. Next, a matrix convolution operation allows for the true introduction of bit randomness in the resulting encrypted images. The authors of [19] introduce a pool of chaotic maps, namely, Arnold, Logistic, Henon, Duffing and Tent maps. Then, based on the properties of the image to be encrypted, as well as other parameters, one of maps from the pool would be selected for use. This map is then employed in combination with DNA sequence operations to carry out image encryption. Next, a Mandelbrot set based algorithm is utilized to carry out bit confusion on each of the RGB channels of the encrypted image. DNA coding is also utilized by the authors of [41], in combination with a six-dimensional discrete hyperchaotic system. Their proposed algorithm carries out multiple rounds of diffusion encryption.

The carried out literature review reveals that many image encryption algorithms have already been proposed, utilizing one or more chaotic maps. However, it is clear that there is a sheer redundancy of the maps being employed, as well as their combinations. Furthermore, it is clear that to design algorithms suitable for real-time image encryption applications, the literature is redundant with algorithms that either carry out confusion or diffusion, but not both. Thus, sacrificing security and robustness. In this paper, the main contributions are as follows:

1) A color image encryption algorithm is proposed, utilizing 2 keys and a combination of 1D and MD chaotic functions, as well as the KAA map.
2) In order to reach a heightened level of security, the proposed algorithm utilizes both confusion and diffusion, satisfying Shannon's theories [5].
3) The proposed algorithm is tested against a number of visual, statistical and differential attacks, in order to measure its performance in terms of efficiency, robustness and resistivity to cryptanalysis.

4) By employing 2 keys and 9 variables, the key space can be enlarged to 2^{478}, resisting brute-force attacks.
5) The proposed algorithm is shown to pass all the tests of the NIST SP 800 analysis suite.

The rest of this paper is organized as follows: Section II provides the preliminary mathematical concepts employed in the proposed algorithm. Section III describes the methodology of the proposed algorithm. Section IV carries out the performance evaluation and presents the results of the computations in relation to the various visual, statistical, differential and brute-force analyses. Finally, Section V draws the conclusions of this paper and suggests some future research directions.

II. PRELIMINARY OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The proposed image encryption algorithm is based on a number of chaotic maps and a mathematical transformation. These are presented next.

A. THE KAA MAP

In physics, symmetry transformations keep physical quantities invariant [8], [9], [28]. Each symmetry transformation represents a conserved physical quantity or keeps it invariant. Two of the traditional symmetry transformations are: First, the Galilean transformation which is defined as:

$$\begin{aligned} r' &= r + vt \\ t' &= t \end{aligned} \tag{1}$$

where r is the position of the particle in an inertial frame (x, y), r' is the transformed position in a new inertial frame (x', y'), v is a constant in which $|v| \ll c$ is the linear velocity vector of the new frame, and finally t and t' are the invariant time variables.

The Galilean transformation keeps some physical quantities invariant. Among them, is the distance $\Delta r = r_2 - r_1$, that remains invariant under the transformation in the new frame, $\Delta r' = r'_2 - r'_1 = \Delta r = r_2 - r_1$.

Second, the Rotational transformation, which is defined as

$$\begin{aligned} r' = Rr &= \begin{bmatrix} cos\,\theta & -sin\,\theta \\ sin\,\theta & cos\,\theta \end{bmatrix} r, \\ t' &= t, \end{aligned} \tag{2}$$

where θ is a constant rotation angle around the z–axis, for the frame $r = (x, y)$ to rotate into the frame $r' = (x', y')$.

Rotational symmetry transformation also keeps the distance Δr invariant in the new frame. It keeps the position distribution of points unchanged as well. Therefore, the combined symmetry transformation, which is

$$\begin{aligned} r' &= Rr + vt \\ t' &= t \end{aligned} \tag{3}$$

keeps the distance Δr invariant in the new frame and the distribution of the positions of particles (in this case, *pixels*) is maintained.

In the KAA map model, we introduce the transformation:

$$r' = R(\theta(t))r + v(t), \tag{4}$$

where the rotation angle θ is made time (step) dependant $\theta(t)$ and the linear velocity v is no longer constant but made time (step) dependant $v(t)$, as well. The θ and v are polynomial functions that depend on the parameter t. This transformation destroys completely any symmetry of the group of positions r in the initial frame after being transformed into the new frame.

We introduce the KAA map finally as

$$\begin{bmatrix} y' \\ x' \end{bmatrix} = \left[\begin{bmatrix} cos\,\theta & -sin\,\theta \\ sin\,\theta & cos\,\theta \end{bmatrix} \begin{bmatrix} y \\ x \end{bmatrix} + \begin{bmatrix} V_1 \\ V_2 \end{bmatrix} \times t \right] mod\, N, \tag{5}$$

where $mod\, N$ is used to confine the numbers from 0 to 255 which is the minimum and maximum value a pixel can attain.

B. THE 2D LOGISTIC SINE MAP

The 2D Logistic Sine Map (LSM) is a 2 dimensional chaotic map that exhibits excellent chaotic performance because it is derived from both the Logistic map and the Sine map. In [17], the output of the Logistic map was fed as the input of the Sine map and extended to 2D. This results in the mathematical definition of

$$x_{n+1} = sin(\pi a(y_n + 3)x_n(1 - x_n)) \tag{6}$$

and

$$y_{n+1} = sin(\pi a(x_n + 1 + 3)y_n(1 - y_n)). \tag{7}$$

The output are the 2 sequences x_n and y_n while a is the control parameter and $a \in [0, 1]$. In this work, the following parameters are used to generate the chaotic sequence: $x(1) = 0.3$, $y(1) = 0.3$, and $a = 0.9$ as in [17]. Using initial values, their trajectory and Shannon's entropy [33], the authors of [17] estimated the chaotic performance of their 2D LSM. In their work, they provided a trajectory plot of the 2D LSM (Fig. 1 in [17]), showing randomly distributed points in the whole phase plane. This translates into the output of the 2D LSM possessing excellent randomness and ergodicity properties.

C. THE LINEAR CONGRUENTIAL GENERATOR

The linear congruential generator (LCG) was first published in 1960 by Thomson and Rotenberg [31]. It is one of the best PRNGs that provide fast software and hardware implementations [22]. This is because a LCG requires minimal memory to retain state. Evidence of the LCG's statistical superiority as a PRNG is that a 96-bit LCG is compliant with (i.e. passes) the most rigorous BigCrush suite [30]. Here, it is used to generate a sequence of integers from 1 to $(m - 1)$, and is mathematically defined as

$$X_n = (aX_{n-1} + c) mod\, m, \tag{8}$$

where a is a control parameter as in [36].

D. THE BERNOULLI MAP

The Bernoulli chaotic map is a one dimensional chaotic map that is defined from the range $-A$ to A. It is one example of strongly chaotic functions that display exponential decay of correlation to their equilibrium values. Not only is it easy to compute, but also provides much desired properties of chaotic behavior needed for image encryption. The Lyapunov exponent of the Bernoulli map is $log2$. Being an exact system (i.e. mixing and ergodic), after only a small number of iterations, the Bernoulli map when applied with 2 different sets of initial conditions, results in very different trajectories [10]. It is mathematically defined as

$$x(n+1) = \begin{cases} (Bx(n)) - A, & -A < x < 0, \\ (Bx(n)) + A, & 0 < x < A, \end{cases} \tag{9}$$

where the sequence is generated with the following parameters: $A = 0.5, B = 1.75$ and $x(1) = (B \times 0.25) - A$. Therefore, the range of the generated chaotic system is from $-1/2$ to $1/2$ as in [12].

E. THE TENT MAP

The Tent map is also a chaotic one dimensional map that displays a good chaotic sequential behaviour. Similar to the Bernoulli map, it has a Lyapunov exponent of $log2$ [10], but unlike the Bernoulli map, the $x-$correlation function for the Tent map is $\delta-$correlated. It is mathematically expressed as

$$x(n+1) = \begin{cases} C(x(n)), & 0 < x < 1/2 \\ C(1 - x(n)), & 1/2 < x < 1 \end{cases} \tag{10}$$

where the sequence is generated with the parameters $C = 1.5$ and $x(1) = 0.5$, as in [39].

III. METHODOLOGY OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

A. THE ENCRYPTION ALGORITHM

The proposed image encryption algorithm is implemented over a number of steps, as follows.

1) A color image of dimensions $N \times N$, where for example $N = 256$, is loaded and color-separated into its 3 RGB channels.
2) Each channel's pixels are then shuffled using the sequence generated from the KAA map, thus inducing diffusion in the image pixels.
3) Two encryption keys are generated. The first key is generated using the 2D Sine Logistic Map and the Linear Congruential Generator. It consists of a 256×256 bits matrix.
   - The floating point output sequences, x and y, resulting from the 2D Sine Logistic Map are then converted to 64–bit by utilizing the IEEE–754 double precision conversion. The control parameter a is converted to 64–bit in the same manner. Nevertheless, it is shortened, such that only the first 44 bits are employed.
   - Two sequences, $L1$ and $L2$, are generated through the use of the linear congruential generator. These employ the parameters, respectively: $L1_0 = 3,538,644,446, a_L1 = 27, c = 0, m = 2^{52} - 1$ and $L2_0 = 2,700,000, a_L2 = 37, c = 1, m = 2^{32} - 1$. The generated integer sequences $L1$ and $L2$ are converted to 52 and 32 bits, respectively.
   - Hence, the first key is the concatenation of the bits of the x, y, a, $L1$ and $L2$ which is $64 + 64 + 44 + 52 + 32$ resulting in a 256×256 bits matrix.
4) Each channel's shuffled pixels bits are reshaped to $8 \times [256 \times 256]$ resulting in 8 sub matrices in each channel to be XORed with the first key generated in a bit–by–bit manner.
5) The Bernoulli and the Tent chaotic maps are then employed to generate the second key. This key is made up of a 65536×8 matrix.
   - The decimal number sequence generated from the Bernoulli map is binarized through a simple decision rule. This is carried out by setting a threshold and comparing each element against it. If an element is greater than the threshold, it is assigned a value of 1, otherwise it is assigned a value of 0. The threshold is set to be 0. Furthermore, the length of the output bit sequence is 32768×8.
   - In a similar fashion a bit sequence is obtained from the Tent map. However, the threshold is set to have a value of 0.5. The length of the output bit sequence is 32768×8.
   - The second key is the concatenation of both sequences. This generate a 65536×8 bit matrix which is XORed again in a bit–by–bit manner with each of the RGB channels of the image.

Flow charts illustrating the generation of each of the encryption keys, as well as the proposed algorithm, are shown in Fig. 1, Fig. 2 and Fig. 3, respectively.

B. THE DECRYPTION ALGORITHM

The decryption algorithm follows the reverse order of steps of the encryption algorithm, generating and utilizing the same set of keys.

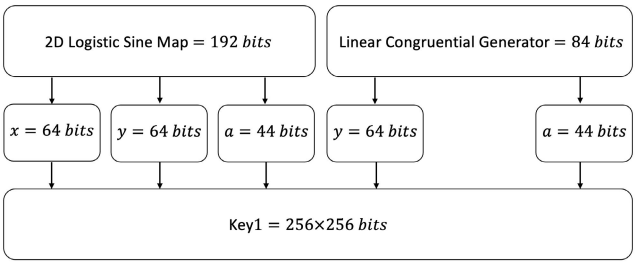


FIGURE 1. Flow chart showing the generation of the first encryption key, based on the 2D LSM and the LCM.

IV. SECURITY ANALYSIS AND NUMERICAL RESULTS

This section provides the computation of the various metrics utilized to gauge the performance of the proposed image

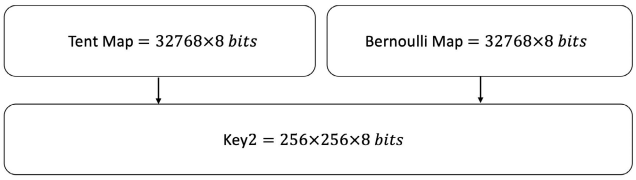


FIGURE 2. Flow chart showing the generation of the second encryption key, based on the Tent and Bernoulli chaotic maps.

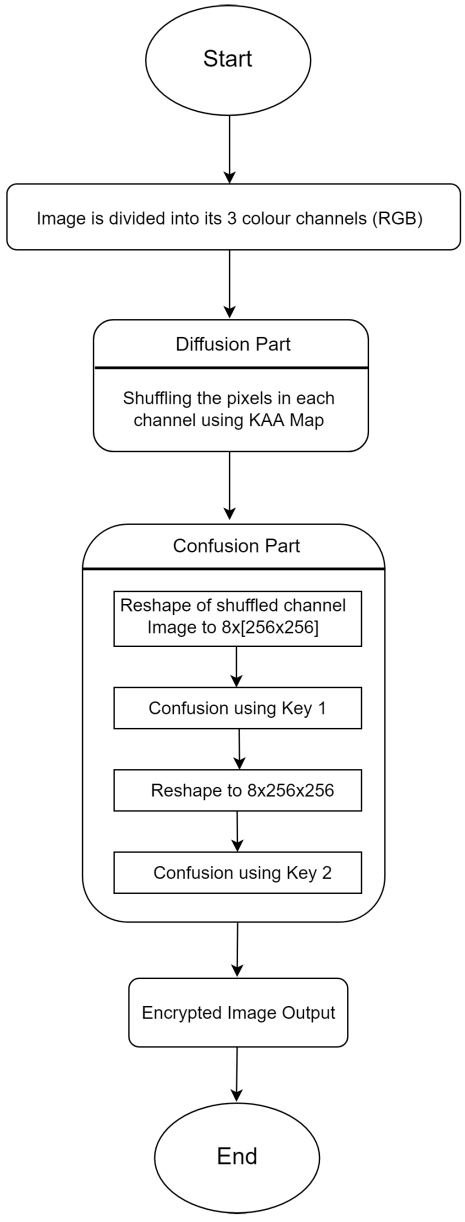


FIGURE 3. Flow chart showing the encryption process.

encryption algorithm. A number of images popular in the image processing community are employed. Those are Lena, Mandrill and Peppers, all of dimensions 256×256. Comparisons with counterpart algorithms from the literature are also carried out.

FIGURE 4. Plain lena image.

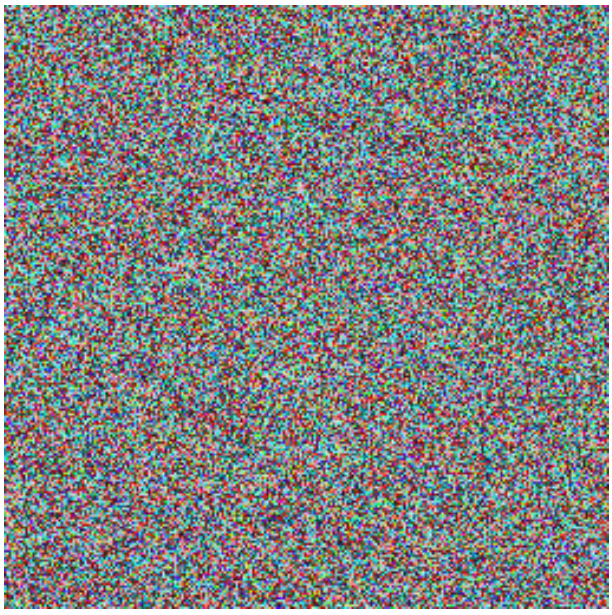


FIGURE 5. Encrypted lena image.

A. VISUAL AND HISTOGRAM ANALYSES

The first and most simple metric for evaluating any image encryption algorithm is through an assessment by the human visual system (HVS). Fig. 4 and Fig. 5 respectively show the plain and encrypted images of Lena. Fig. 6 and Fig. 7 respectively show the plain and encrypted images of Mandrill, while Fig. 8 and Fig. 9 respectively show the plain and encrypted images of Peppers. It is clear that the images in Fig. 5, Fig. 7 and Fig. 9 represent unintelligible data.

The second visual evaluation metric is the image histogram. In the context of data encryption, an image histogram is a description of the probability density function for

FIGURE 6. Plain mandrill image.

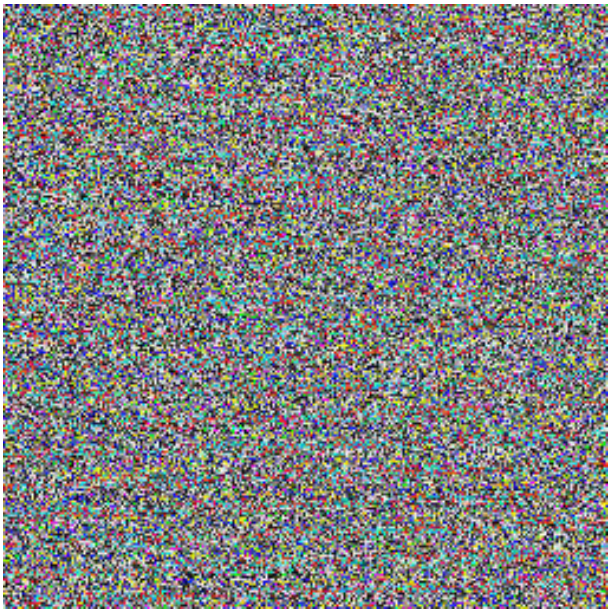


FIGURE 7. Encrypted mandrill image.

FIGURE 8. Plain peppers image.

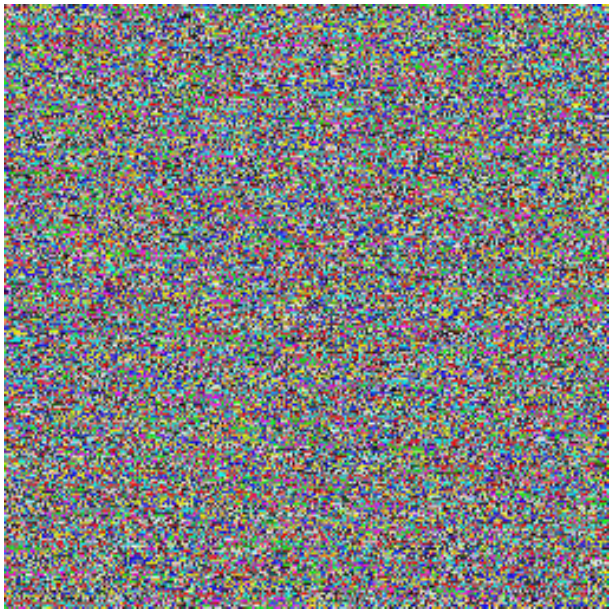


FIGURE 9. Encrypted peppers image.

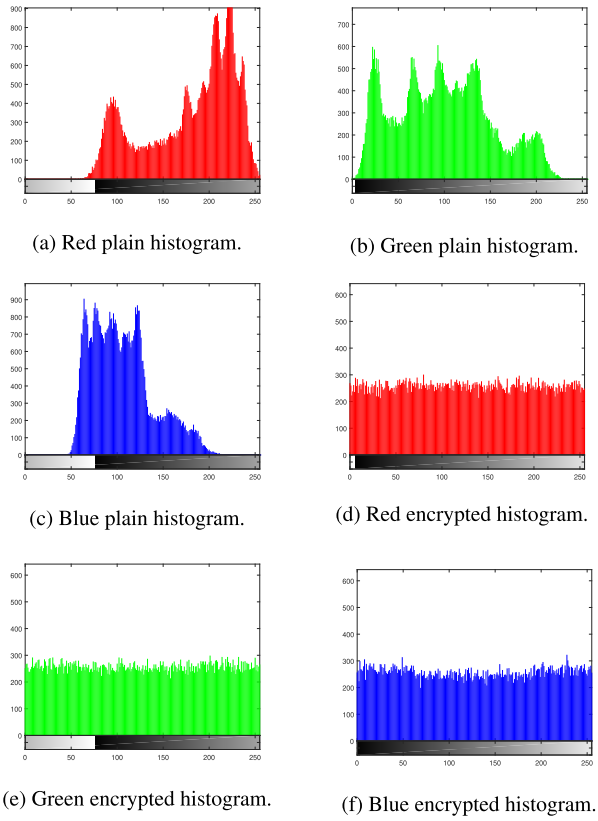
its pixels. A strong encryption scheme appears in the histogram as a uniform distribution among an image's gray levels, hiding any statistical characteristics in the image. This can be interpreted in Fig. 10, which proves the difficulty of information retrieval from encrypted images and thus the resistance of the proposed encryption algorithm against statistical attacks.

B. INFORMATION ENTROPY

Information entropy is used as a metric to evaluate an image based on the randomness of the distribution of its gray pixels. Equation (11) shows how it is calculated for an image, where $p(m_i)$ represents the probability of occurrence of each symbol m in the total number of M symbols in an image.

$$H(m) = \sum_{i=1}^{M} p(m_i) \log_2 \frac{1}{p(m_i)}. \tag{11}$$

Ideally, for a randomly encrypted gray scale image with 256 symbols, its entropy value would be 8, and is reduced with less random encryption [48]. This is shown in Table 1, where information entropy is calculated for each of the RGB channels of the 3 test images, all exhibiting values greater



(a) Red plain histogram. (b) Green plain histogram. (c) Blue plain histogram. (d) Red encrypted histogram. (e) Green encrypted histogram. (f) Blue encrypted histogram.

FIGURE 10. Image histogram of plain and encrypted Lena image.

TABLE 1. Entropy values of the RGB channels of different images.

Image	Channels	Entropy values
Lena	Red	**7.9972**
	Green	7.9965
	Blue	7.9962
Peppers	Red	7.9966
	Green	7.9975
	Blue	**7.9976**
Baboon	Red	7.9965
	Green	7.9963
	Blue	**7.9967**

TABLE 2. Comparison of entropy values of the Lena image RGB channels.

Algorithm	Entropy values of channels		
	Red	Green	Blue
Proposed algorithm	7.9972	7.9965	7.9963
[15]	**7.9994**	**7.9994**	**7.9993**
[20]	7.9973	7.9972	7.9975
[37]	7.9991	7.9954	7.9963
[46]	7.9948	7.9958	7.9950

than 7.99. A comparison with the literature for this metric is also provided in Table 2 and Table 3, where a comparable or superior performance is calculated for our proposed image encryption algorithm, as an average value, or as a separate value for each of the RGB channels, respectively.

TABLE 3. Comparison between the entropy values of the Lena image of the proposed algorithm and different schemes in the literature, of dimensions 256 × 256.

Algorithm	Entropy value
Proposed	7.9987
[4]	7.9984
[19]	7.9992
[20]	7.9990
[46]	7.9985
[51]	**7.9991**

TABLE 4. MSE and PSNR values of different image RGB channels.

Image	Channel	MSE	PSNR
Lena	Red	**10659.2428**	**7.8535**
	Green	9077.2362	8.5513
	Blue	7214.8869	9.5485
Peppers	Red	8049.5736	9.0731
	Green	11016.5437	7.7104
	Blue	**11032.9150**	**7.7039**
Baboon	Red	8464.4954	8.8547
	Green	7479.9641	9.3918
	Blue	**9104.1924**	**8.5384**

C. MEAN SQUARED ERROR

The Mean Squared Error (MSE) is one of the popular metrics used for evaluating the error between original and encrypted images in order to assess the reliability of any encryption algorithm. It is calculated as shown in (12) by squaring the difference between the pixel of the plain image $P_{(i,j)}$ and the encrypted image $E_{(i,j)}$ for all $M \times N$ pixels in the image, then dividing the total squared error for all pixels by their count. Higher MSE values indicate better resilience of an encryption algorithm against statistical attacks.

$$MSE = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P_{(i,j)} - E_{(i,j)})^2}{M \times N}. \tag{12}$$

D. PEAK SIGNAL TO NOISE RATIO

Based on the MSE, the Peak Signal to Noise Ratio (PSNR) is another performance metric that evaluates the quality of encryption algorithms. As shown in (13), the PSNR is calculated by evaluating the log value of the ratio between the square of the maximum pixel value I_{max} to the MSE, where I_{max} is ideally equal to 255. Since PSNR and MSE are inversely proportional, lower PSNR values indicate better resilience of an encryption algorithm.

$$PSNR = 10 \log \left(\frac{I_{max}^2}{MSE} \right). \tag{13}$$

Table 4 shows the MSE and PSNR results of our proposed encryption algorithm for different images. In addition, comparison with the state of the art literature is given in Table 5 and Table 6 for the MSE and PSNR, respectively. The results show that our proposed algorithm's MSE and PSNR values are superior to [47], comparable to [3], underperforming those of [20].

TABLE 5. MSE values comparison of different images.

	Proposed	[20]	[47]	[3]
Lena	8983.7886	**10869.73**	4859.03	8888.88
Peppers	10033.0116	–	6399.05	**10092.3**
Mandrill	8349.5506	**10930.33**	7274.44	8295.21

TABLE 6. PSNR values comparison of different images.

	Proposed	[20]	[47]	[3]
Lena	8.6510	**7.7677**	11.3	8.64233
Peppers	8.1624	–	10.10	**8.09089**
Baboon	8.9283	**7.7447**	9.55	8.94253

E. CORRELATION COEFFICIENT ANALYSIS

Analysis of correlation coefficient, r, is another metric that is highly important in evaluating the performance of an encryption algorithm. The correlation coefficient between 2 pixels x and y is calculated as shown in (14) to (17); resulting in a value that varies between -1 and 1. For an encryption scheme to be resilient against statistical attacks, the correlation coefficient between adjacent pixels in all three directions, horizontally (H), vertically (V) and diagonally (D), should be close to zero to indicate no correlation. Otherwise, values close to -1 indicate strong negative correlation and values close to 1 indicate strong positive correlation, which make it feasible for an encrypted image to be exposed by statistical attacks.

Table 7 clearly shows a strong correlation between the adjacent pixels of the plain image. On the other hand, from Table 8, it is clear that adjacent pixels of the encrypted image have no correlation what so ever, in each of the H, V, or D directions. These differences in values between Table 7 and Table 8 can be visually confirmed by inspecting the sub-figures of Fig. 11. It is clear the first 3 sub-figures show a strong correlation between their pixels, unlike the lack of correlation in the last 3 sub-figures. The same pixel correlation behavior is also noticed when examining the correlation plots for each of the separate RGB channels of the Lena image in Fig. 12, Fig. 13 and Fig. 14. Furthermore, Table 9 and Table 10 show that the computed correlation coefficient values are comparable to counterpart schemes from the literature. Finally, Fig. 15 and Fig. 16 provide 3D plots for the correlation coefficient matrices of the plain and encrypted Lena images, respectively. While Fig. 15 displays values concentrated in a diagonal fashion, it is clear that Fig. 16 shows total random distribution of the values.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{15}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{16}$$

TABLE 7. Correlation coefficients of adjacent pixels in plain images. Shown here in 3 directions, horizontal, diagonal and vertical.

Image	H	D	V
Lena	0.96734	0.94821	0.98276
Peppers	0.95595	0.95371	0.97939
Mandrill	0.92203	0.87049	0.90303

TABLE 8. Correlation coefficients of adjacent pixels in encrypted images. Shown here in 3 directions, horizontal, diagonal and vertical.

Image	H	D	V
Lena	**0.00144**	−0.00151	0.00795
Peppers	**−0.00021**	0.00027	0.00128
Mandrill	**−0.00004**	−0.00021	0.00039

and

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i). \tag{17}$$

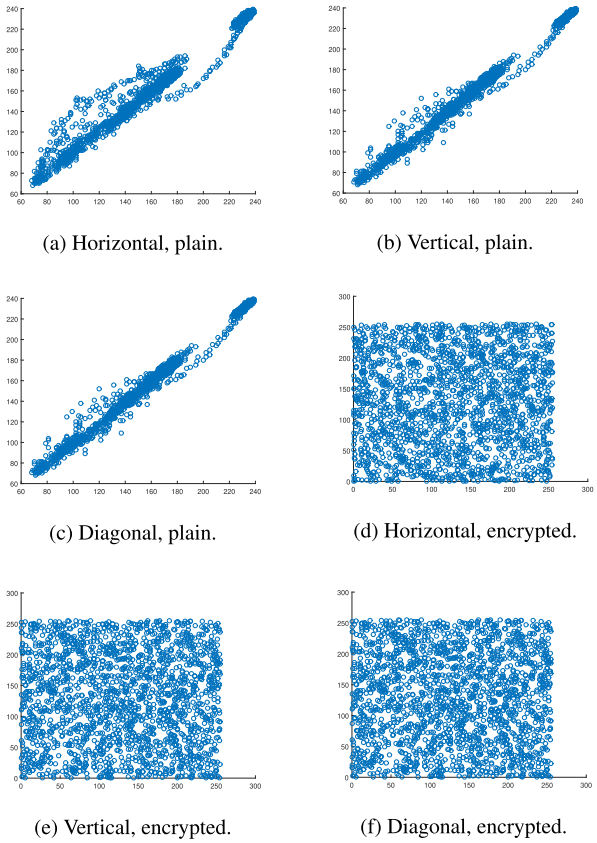
Another interesting manner to examine the correlation between adjacent pixels is to examine the Fourier Transform of a plain image and its encrypted version. First off, the Fourier transform of a square image $f(i,j)$ is expressed mathematically as

$$F(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)e^{-i2\pi(\frac{ki}{N}+\frac{li}{N})}, \tag{18}$$

such that $f(a,b)$ is the image representation in the spatial domain, with the exponential term being the basis function that corresponds to each point $F(k,l)$ in the Fourier space. The basis functions here are the sine and cosine waves with increasing frequencies. This translates into $F(0,0)$ being the DC-component of the image and thus corresponds to average brightness, while $F(N-1,N-1)$ would represent the highest frequency. Fig. 17a shows the plain Lena image where the Fourier transform is applied. It is clear that the center of the image represents pixels with high correlation, evident through the plus-sign form in the middle of the image. This is due to the plain image having special features such as edges for example. On the other hand, Fig. 17b shows the Fourier transform applied to an encrypted Lena image, with a rather uniform distribution of values due to the lack of any special features. This corresponds to no correlation between adjacent pixels.

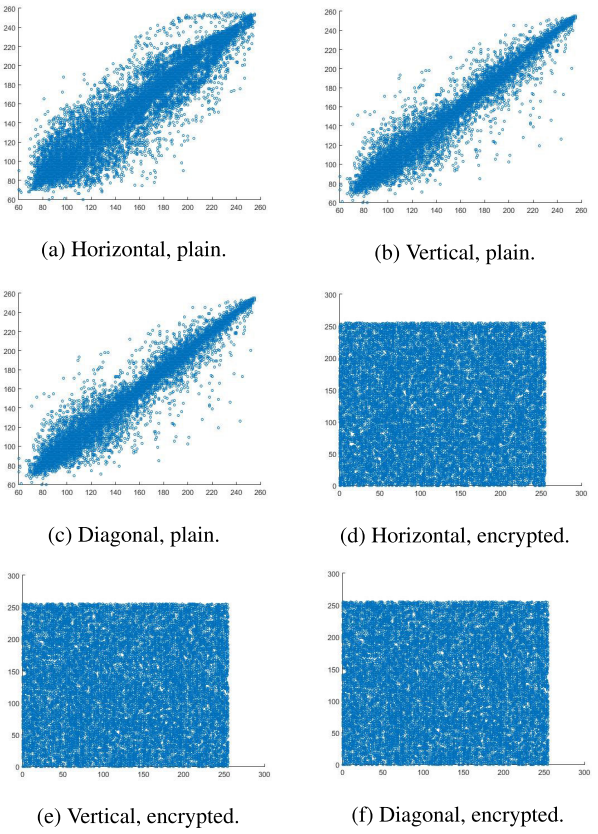
F. KEY SPACE ANALYSIS

In our 2 utilized keys we have a total of 9 variables and we consider in this paper that the largest machine precision is 10^{-16}, which leads to our proposed image encryption algorithm to effectively have a key space that is larger than $10^{9\times16} = 10^{144} \approx 2^{478}$, and achieve theoretical nonviolent cracking [27]. Table 11 compares the achieved key space of the proposed image encryption algorithm with those of its counterparts from the literature. It is clear that our achieved key space is superior to other values in the table,



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain. (d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 11. Correlation coefficient diagram of the plain and encrypted Lena images.



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain. (d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 12. Correlation coefficient diagram of the plain and encrypted red channel of Lena image.

TABLE 9. Correlation coefficient comparison of plain and encrypted Lena image colour channels with the literature.

Lena					
RGB	CC	Plain	Proposed Enc.	[50] Enc.	[19] Enc.
R	H	0.95722	**0.00073**	0.001365	0.0021
	D	0.93389	0.00311	**0.000232**	−0.0026
	V	0.97889	−0.00508	0.004776	**0.0018**
G	H	0.94321	**−0.00054**	0.003294	−0.0006
	D	0.91931	0.00076	0.004807	**0**
	V	0.97137	0.00331	**0.000579**	0.0004
B	H	0.92845	**0.00147**	0.002060	−0.005
	D	0.90068	**−0.00147**	0.004043	−0.0104
	V	0.95593	0.006219	**0.000194**	0.001

TABLE 10. Correlation coefficients comparison between plain and encrypted Lena images.

Algorithm	Horizontal	Diagonal	Vertical
Proposed	0.00175	**0.000013**	**0.000014**
[20]	0.0054	0.0054	0.0016
[26]	0.001862	0.003768	0.000710
[29]	0.0022	−0.0017	0.0001
[41]	**0.000199**	0.003705	−0.000924
[42]	0.0029	0.0045	0.0001
[43]	0.0082	−0.0012	−0.0128

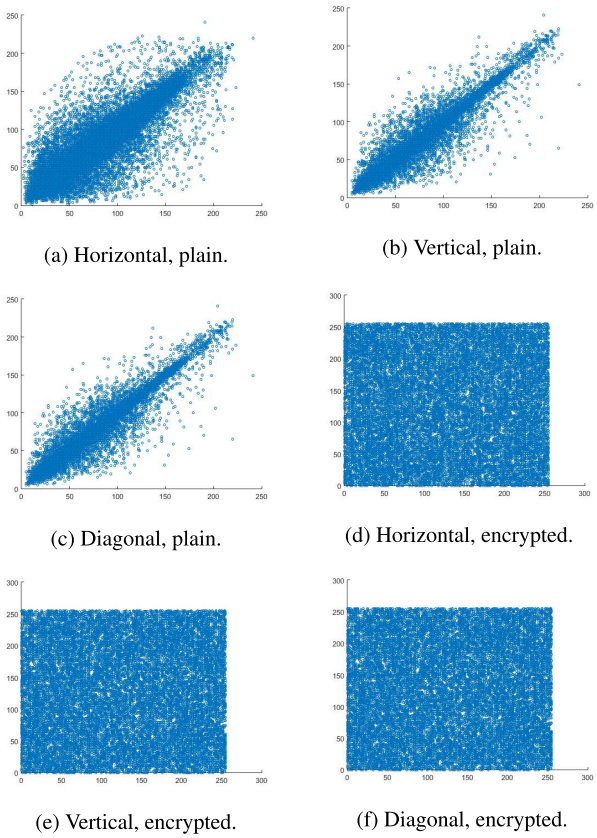
with the exception of the algorithm proposed in [19] which reportedly has a key space given by $(2 \times 10^{15})^3 \times 10^2 \times 256^{65,536\times 3} \approx \infty$.

TABLE 11. Key space values comparison.

Algorithm	Key space
Proposed	$\mathbf{10^{144} \approx 2^{478}}$
[3]	10^{128}
[4]	2^{299}
[11]	2^{256}
[15]	10^{169}
[16]	2^{219}
[25]	2^{128}
[41]	2^{187}
[38]	10^{94}
[45]	2^{256}
[19]	∞

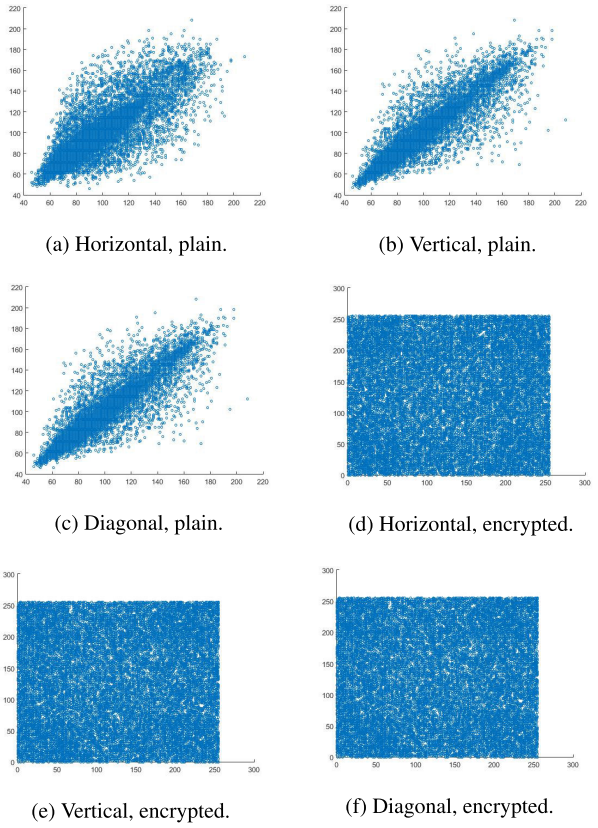
G. DIFFERENTIAL ATTACK ANALYSIS

Differential attacks are carried out by introducing small changes to a plain image, then obtaining the corresponding encrypted image, before and after the said modification. Next, an attempt to compute the key through data analysis is carried out. Thus, a secure image encryption algorithm should allow even the simplest of changes to the plain image to lead to a tremendous change in the resulting encrypted image. The 2 metrics that can be best utilized to assess an image encryption algorithm's resistance to differential attacks are the number of pixel changing rate (NPCR) and the unified average change intensity (UACI). The mathematical



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain. (d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 13. Correlation coefficient diagram of the plain and encrypted green channel of Lena image.



(a) Horizontal, plain. (b) Vertical, plain. (c) Diagonal, plain. (d) Horizontal, encrypted. (e) Vertical, encrypted. (f) Diagonal, encrypted.

FIGURE 14. Correlation coefficient diagram of the plain and encrypted blue channel of Lena image.

expression for NPCR is given as

$$NPCR = \frac{\sum_{i,j} D_{i,j}}{M \times N} \times 100, \tag{19}$$

where $D_{i,j}$ is given by

$$D_{i,j} = \begin{cases} 0 & C_{1(i,j)} = C_{2(i,j)} \\ 1 & C_{1(i,j)} \neq C_{2(i,j)}. \end{cases} \tag{20}$$

The NPCR is a calculation that results in the number of pixels which are different between a plain and an encrypted image. The UACI is mathematically expressed as

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255}, \tag{21}$$

where $C_{1(i,j)}$ and $C_{2(i,j)}$ are 2 images of dimensions $M \times N$. It is a calculation that reflects the difference in the average intensity between a plain and an encrypted image. Table 12 and Table 13 provide the achieved NPCR and UACI values of the Lena image. As shown, the achieved NPCR values are all above 99%. However, while the UACI should be about 33.35%, a few of the values are close enough but not exactly that percentage. Moreover, the achieved results are comparable to those resulting from counterpart algorithms from the literature.

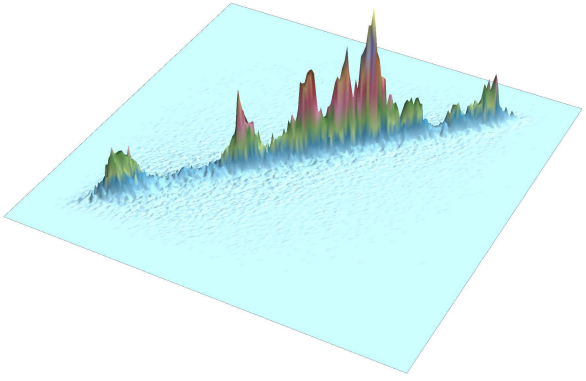


FIGURE 15. 3D plot of the correlation coefficient matrix of the plain Lena image.

TABLE 12. NPCR values for the RGB channels of the Lena image.

RGB	Proposed	[34]	[3]	[15]	[20]
R	99.6254	**99.6355**	99.6109	99.6065	99.58
G	99.6254	**99.6256**	99.6109	99.6147	99.56
B	99.6254	99.6159	**99.6375**	99.6235	99.64

H. MEAN ABSOLUTE ERROR

The Mean Absolute Error (MAE) is another metric that is utilized to evaluate how an encryption algorithm performs

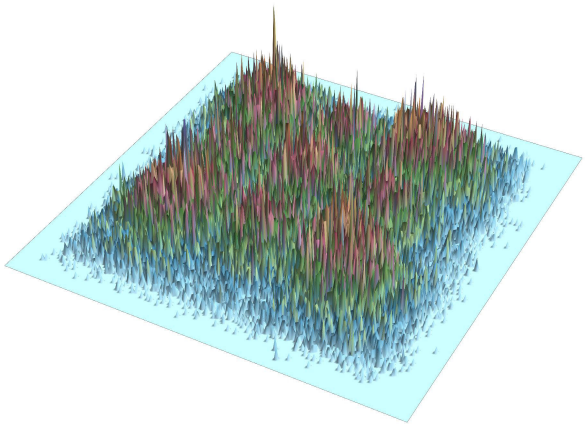


FIGURE 16. 3D plot of the correlation coefficient matrix of the encrypted Lena image.

TABLE 13. UACI values for the RGB channels of the Lena image.

RGB	Proposed	[34]	[3]	[15]	[20]
R	33.0704	**33.4657**	33.4158	33.4108	33.27
G	30.7620	33.4552	30.3902	**33.4653**	33.36
B	27.8720	**33.4550**	33.2420	33.4901	33.50

TABLE 14. MAE values comparison of different images.

Image	Proposed	[20]	[21]
Lena	77.99158	**87**	77.35
Peppers	**81.83799**	–	74.71
Baboon	75.46050	**92**	73.91

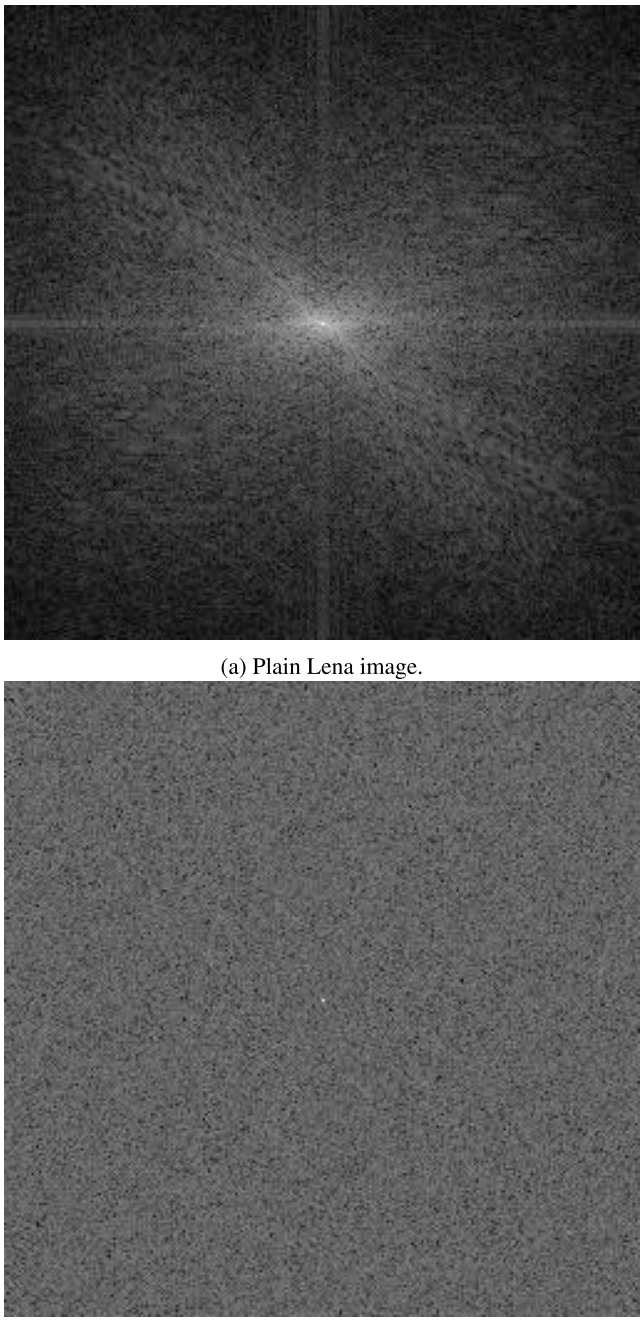
against differential attacks. The MAE measures the average difference between a pixel of the plain image $P_{(i,j)}$ and that of its encrypted version $E_{(i,j)}$ for all $M \times N$ pixels in an image. It is mathematically expressed as

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} P_{(i,j)} - E_{(i,j)}. \tag{22}$$

The higher the value of the MAE the more the proposed encryption algorithm would be robust to differential attacks. Table 14 shows how our computed MAE values compare to those of counterpart schemes. It is clear that our MAE values are lower bounded by those of [21] and upper bounded by those of [20].

I. ENCRYPTION TIME ANALYSIS

We use the time needed for encryption as a measure of the complexity of the proposed algorithm, as well as its suitability for utilization in real time applications. Table 15 shows the encryption time of 3 images having dimensions of 256 × 256, while Table 16 provides an encryption time comparison among the proposed algorithm and its counterparts from the literature. Our proposed algorithm's encryption time is low compared to [16], and [44], high compared to [4], [49], and [14] while similar to [3]. However, it is important to note that the provided encryption times in Table 16 are achieved utilizing machines with different processing powers and memories.



(a) Plain Lena image.

(b) Encrypted Lena image.

FIGURE 17. Fourier transform of the plain and encrypted Lena images.

TABLE 15. Encryption time of the proposed algorithm for various images.

Image	Time [s]
Lena	2.750966
Baboon	**2.637110**
Peppers	2.793215

TABLE 16. Encryption time comparison of the Lena image.

Algorithm	Time [s]	Machine specs. (CPU and RAM)
Proposed	2.750966	3.4 GHz Intel® Core™ i7, 8 GB
[3]	2.582389	2.9 GHz Intel® Core™ i9, 32 GB
[4]	**0.25**	**N/A**
[14]	1.1168	3.4 GHz Intel® Core™ i7, 8 GB
[16]	3.45	N/A
[44]	4.98	2.5 GHz AMD®, 4 GB
[49]	1.112	3.4 GHz Intel® Core™ i3, 4 GB

TABLE 17. NIST analysis on the RGB color channels of an encrypted Lena image.

Test Name	Red	Green	Blue	Remarks
Frequency	0.969154	0.116031	0.642620	Success
Block Frequency	0.537532	0.844623	0.603790	Success
Run	0.062648	0.253088	0.132307	Success
Long runs of ones	0.732551	0.131164	0.089006	Success
Rank	0.729652	0.085249	0.903271	Success
Spectral FFT	0.686934	0.605100	0.104216	Success
Non overlapping	0.989725	0.963289	0.428404	Success
Overlapping	0.515821	0.064806	0.014539	Success
Universal	0.721258	0.124221	0.019760	Success
Serial	0.955458	0.402424	0.149208	Success
Serial	0.957799	0.162185	0.385400	Success
Approx. entropy	0.432168	0.161315	0.399786	Success
Cum. sums forward	0.750452	0.199999	0.120316	Success
Cum. sums reverse	0.714170	0.122212	0.313745	Success

J. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ANALYSIS

One good measure of randomness in encrypted images is that introduced by the National Institute of Standards and Technology (NIST), commonly known as the *NIST SP 800 analysis*. The NIST analysis is a suite of tests carried out on a bitstream to check for its behavior as a PRNG. For a bitstream to pass each of those tests its probability, or $p-$value should be greater than 0.01. Here, we test a lengthy sequence of bits, obtained from the concatenation of the rows of a large encrypted image, using our proposed algorithm, and prove that the bit sequence does in fact pass the NIST analysis. For illustration purposes, we display the results of a NIST analysis in Table 17, as carried out on each of the RGB color channels of a Lena image of dimensions 256×256. It is clear that all of the values in Table 17 are greater than 0.01, showcasing the success of the proposed image encryption algorithm at passing the NIST analysis.

V. CONCLUSION AND FUTURE WORKS

In this paper, we proposed a color image encryption algorithm based on a number of chaotic maps, as well as the derived KAA map. The various maps were utilized to implement Shannon's ideas of confusion and diffusion for better cryptographic security. The performance of the proposed algorithm was evaluated using various metrics, including a visual comparison, a histogram analysis, information entropy, MSE, PSNR, a correlation coefficient analysis, a differential attack analysis (including NPCR, UACI, MAE), a key space analysis, an execution time analysis, as well as a NIST analysis. The outcome of the various conducted analyses showcase the ability of the proposed image encryption algorithm to withstand various cryptanalytic attacks, including visual, statistical, differential and brute-force attacks. Finally, upon comparing the values of the various metrics of the proposed algorithm, it was shown to exhibit a comparable or superior performance when compared to those computed for its counterparts from the literature. Superior performance is especially exemplified both by the near-null pixel correlation coefficients of the encrypted images as well as the very large key space.

REFERENCES

[1] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany, and E. A. A. Hagras, "Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves," *IEEE Access*, vol. 8, pp. 57733–57748, 2020.

[2] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Image encryption through Lucas sequence, S-Box and chaos theory," in *Proc. 8th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Dec. 2021, pp. 77–83.

[3] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, S-Box and the Lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, Feb. 2022.

[4] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19853–19873, Jul. 2020.

[5] D. R. Anderson, *Model Based Inference in the Life Sciences: A Primer on Evidence*, vol. 31. New York, NY, USA: Springer, 2008.

[6] B. Arpacı, E. Kurt, K. Çelik, and B. Ciylan, "Colored image encryption and decryption with a new algorithm and a hyperchaotic electrical circuit," *J. Electr. Eng. Technol.*, vol. 15, no. 3, pp. 1413–1429, May 2020.

[7] D. Arroyo, J. Diaz, and F. B. Rodriguez, "Cryptanalysis of a one round chaos-based substitution permutation network," *Signal Process.*, vol. 93, no. 5, pp. 1358–1364, May 2013.

[8] M. Bañados and I. Reyes, "A short review on Noether's theorems, gauge symmetries and boundary terms," *Int. J. Modern Phys. D*, vol. 25, no. 10, Sep. 2016, Art. no. 1630021.

[9] T. Bertschinger, N. Flowers, S. Moseley, C. Pfeifer, J. Tasson, and S. Yang, "Spacetime symmetries and classical mechanics," *Symmetry*, vol. 11, no. 1, p. 22, Dec. 2018.

[10] D. J. Driebe, *Fully Chaotic Maps and Broken Time Symmetry*, vol. 4. New York, NY, USA: Springer, 1999.

[11] H. Gao and X. Wang, "Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position," *IEEE Access*, vol. 9, pp. 105627–105640, 2021.

[12] H. Garcés and B. C. Flores, "Statistical analysis of Bernoulli, logistic, and tent maps with applications to radar signal design," *Proc. SPIE*, vol. 6210, May 2006, Art. no. 62100G.

[13] B. Ge, X. Chen, G. Chen, and Z. Shen, "Secure and fast image encryption algorithm using Hyper-Chaos-Based key generator and vector operation," *IEEE Access*, vol. 9, pp. 137635–137654, 2021.

[14] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.

[15] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools Appl.*, vol. 79, pp. 1–19, Mar. 2019.

[16] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020.

[17] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "Image encryption using 2D logistic-sine chaotic map," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2014, pp. 3229–3234.

[18] L. M. Jawad, "A new scan pattern method for color image encryption based on 3D-Lorenzo chaotic map method," *Multimedia Tools Appl.*, vol. 80, no. 24, pp. 33297–33312, Oct. 2021.

[19] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102428.

[20] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Sep. 2019.

[21] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Comput. Appl.*, vol. 26, no. 5, pp. 1137–1148, Jul. 2015.

[22] D. E. Knuth, *The Art of Computer Programming. Volume 1: Fundamental Algorithms. Volume 2: Seminumerical Algorithms*. Providence, Rhode Island: Bulletin of the American Mathematical Society, 1997.

[23] V. Kumar and A. Girdhar, "A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 3749–3773, 2021.

[24] M. Kumari and S. Gupta, "Performance comparison between chaos and quantum-chaos based image encryption techniques," *Multimedia Tools Appl.*, vol. 80, no. 24, pp. 33213–33255, Oct. 2021.

[25] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on logistic map and dynatomic modular curve," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8911–8938, Apr. 2018.

[26] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Process.*, vol. 113, pp. 104–112, Aug. 2015.

[27] H. Liu, X. Wang, and A. Kadir, "Chaos-based color image encryption using one-time keys and choquet fuzzy integral," *Int. J. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 1, pp. 1–10, Feb. 2014.

[28] K. S. Mallesh, S. Chaturvedi, V. Balakrishnan, R. Simon, and N. Mukunda, "Symmetries and conservation laws in classical and quantum mechanics," *Resonance*, vol. 16, no. 3, pp. 254–273, Mar. 2011.

[29] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, Mar. 2017.

[30] M. E. O'Neill, "PCG: A family of simple fast space-efficient statistically good algorithms for random number generation," Harvey Mudd College, Claremont, CA, USA, Tech. Rep. HMC-CS-2014-0905, Sep. 2014. [Online]. Available: https://www.cs.hmc.edu/tr/hmc-cs-2014-0905.pdf

[31] A. Rotenberg, "A new pseudo-random number generator," *J. ACM*, vol. 7, no. 1, pp. 75–77, Jan. 1960.

[32] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[33] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.

[34] N. Ben Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30993–31019, Dec. 2018.

[35] W. Stallings, *Cryptography & Network Security GE*. London, U.K.: Pearson, 2017.

[36] H.-C. Tang, "An analysis of linear congruential random number generators when multiplier restrictions exist," *Eur. J. Oper. Res.*, vol. 182, no. 2, pp. 820–828, Oct. 2007.

[37] M. Tanveer, T. Shah, A. Rehman, A. Ali, G. F. Siddiqui, T. Saba, and U. Tariq, "Multi-images encryption scheme based on 3D chaotic map and substitution box," *IEEE Access*, vol. 9, pp. 73924–73937, 2021.

[38] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018.

[39] M. V. Harten, "The dynamics of the one-dimensional tent map family and quadratic family," M.S. thesis, Dept. Math. Appl. Math., Faculty Sci. Eng., Univ. Groningen, The Netherlands, 2018.

[40] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019.

[41] Y. Wang, C. Wu, S. Kang, Q. Wang, and V. Mikulovich, "Multi-channel chaotic encryption algorithm for color image based on dna coding," *Multimedia Tools Appl.*, vol. 79, pp. 1–26, Jul. 2020.

[42] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 855–875, Oct. 2017.

[43] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.

[44] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[45] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field ZN," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21803–21821, Aug. 2018.

[46] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, "Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit," *IEEE Access*, vol. 7, pp. 58751–58763, 2019.

[47] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.

[48] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 6, pp. 7841–7869, 2019.

[49] X. Zhang, L. Wang, Y. Wang, Y. Niu, and Y. Li, "An image encryption algorithm based on hyperchaotic system and variable-step Josephus problem," *Int. J. Opt.*, vol. 2020, pp. 1–15, Oct. 2020.

[50] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106040.

[51] C. Zou, Q. Zhang, X. Wei, and C. Liu, "Image encryption based on improved Lorenz system," *IEEE Access*, vol. 8, pp. 75728–75740, 2020.

WASSIM ALEXAN (Senior Member, IEEE) was born in Alexandria, Egypt, in 1987. He received the B.Sc., M.Sc., and Ph.D. degrees in communications engineering and the M.B.A. degree from German University in Cairo (GUC), Egypt, in 2010, 2012, 2017, and 2019, respectively.

He was with the Mathematics Department, from 2010 to 2017. Since 2017, he has been an Assistant Professor with the Faculty of Information Engineering and Technology, GUC, teaching various courses in relation to wireless communications, modulation and coding, digital logic design, circuit theory, and mathematics. He has been an Adjunct Assistant Professor with the Mathematics Department, German International University (GIU), New Administrative Capital, Egypt, since 2019. He is the author or coauthor of more than 60 journal articles and conference papers. His research interests include wireless communications, information security, image, and signal processing.

Dr. Alexan is also a member of the ACM and has been granted the Best Paper Award at the 19th IEEE Conference on Signal Processing Algorithms, Architectures, Arrangements and Applications (SPA 2015), Poznan, Poland, the AEG Writer of the Year Award from the American University in Cairo (AUC), Egypt, in 2019, and the Best Poster Award at the 37th IEEE National Radio Science Conference, Cairo, Egypt, in 2020.

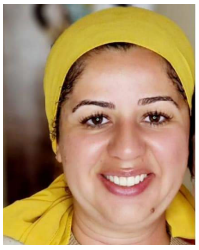
MARWA ELKANDOZ was born in Alexandria, Egypt, in 1995. She received the B.Sc. and M.Sc. degrees in communication engineering from German University in Cairo (GUC), in 2018 and 2021, respectively.

Since 2019, she has been working as a Teaching Assistant with the Physics Department, GUC, where she worked as an Assistant Lecturer, from 2021 to 2022. She published four conference papers and one journal article in the field of data security, including image encryption, audio, and 3D image steganography.

MAGGIE MASHALY (Senior Member, IEEE) received the B.Sc. degree (Hons.) in information engineering and technology and the master's degree in networking from German University in Cairo, Egypt, in 2010 and 2011, respectively, and the Ph.D. degree in cloud computing and computer networks from the University of Stuttgart, Germany, in 2017.

She is currently an Assistant Professor with German University in Cairo, teaching various topics in machine learning, data engineering, and computer networks. She leads multiple research teams in the fields of cloud computing, edge computing, machine learning, and industry 4.0, has numerous publications at well recognized international conferences and journals in the above-mentioned fields, and also acts as a reviewer and a program committee member at many of them.

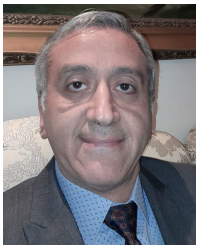
Dr. Mashaly is also a Board Member of the IEEE Women in Engineering Egypt Section.



EMAN AZAB (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electronics and communication engineering from the Faculty of Engineering, Cairo University, in 2006, and the M.Sc. and Ph.D. degrees in electronics engineering from German University in Cairo, Egypt, in 2008 and 2012, respectively.

She did a postdoctoral research at TU Darmstadt, from 2013 to 2015, and working in ion-beam diagnostics with GSI Helmholtzzentrum, Germany. She has been an Assistant Professor with German University in Cairo, teaching various topics in analog, mixed signal electronics, and electrical engineering, since 2016. She leads and is a part of multiple research teams in the fields of sensor technologies, IC design, and industry 4.0. She has numerous publications at well recognized international conferences and journals in the above-mentioned fields.

Dr. Azab is also serving as the Secretary for the IEEE Women in Engineering Egypt Section.



AMR ABOSHOUSHA was born in Cairo, Egypt, in 1967. He received the B.Sc. degree (Hons.) in physics and the M.Sc. degree in theoretical physics from the Science Faculty, Cairo University, in 1988 and 1995, respectively, and the Dr. Rer. Nat. degree in theoretical physics from Friedrich Alexander University Erlangen–Nuerenberg, Germany, in 2001.

From 2002 to 2010, he started to work as a Physics Lecturer with the Physics Department, Science Faculty, Cairo University. During this period, he instructed and supervised various physics courses, such as thermodynamics, electromagnetism, statistical mechanics, computational physics, and optical communications. Since 2010, he has been working as an Assistant Professor with the Physics Department, Faculty of Engineering, German University in Cairo (GUC), teaching different physics related courses to engineering, biotechnology, and pharmacy students. His research interests include the applications of theoretical physics models in different areas, such as information technology and biophysics.

Dr. Aboshousha was a Reviewer of the Physics Exam Committee, High School Certificate, Ministry of Education, from 2004 to 2005.