j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

New Colorful Image Encryption Method Using Triple Chaotic Maps and Grey Wolf Optimization (GWO)

Qutaiba K. Abed[1] and Waleed A. Mahmoud Al-Jawher[2]

[1] *Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq*

[2]*College of Engineering, Uruk University, Baghdad, Iraq.*

phd202130682@iips.edu.iq

Abstract A novel image encryption algorithm employing triple chaotic maps has been developed to address the shortcomings of existing methods in terms of security and efficiency. The algorithm leverages the interconnectivity of color channels in images, using distinct keys to disrupt pixel correlations within each channel. The three chaotic maps utilized URUK, WAM, and Nahrain to generate two sets of keys. The first set is used to shuffle pixel positions, creating scrambled channels. Subsequently, the second set is applied to diffuse these scrambled channels independently. A gray wolf optimization (GWO) algorithm is then employed to further optimize the shuffling process, minimizing pixel correlations and enhancing security. The triple chaotic maps of varying orders contribute to the unpredictability and robustness of the cipher image. A comprehensive security analysis, including entropy, correlation coefficients, and attack resistance, demonstrates the superior performance of the proposed method compared to existing image encryption algorithms

Crossref 10.36371/port.2024.3.11

Keywords: *GWO, WAM chaotic map, URUK chaotic map, Nahrain chaotic map*

1. INTRODUCTION

The rapid advancement of digital technologies has led to a significant increase in the transmission of digital images, which are crucial in various fields [1]. However, these images often contain sensitive personal or confidential information vulnerable to unauthorized access [2]. Protecting this information is essential for individuals and countries alike. To address this challenge, various methods have been developed to secure digital images, including encryption [3, 4], steganography [5, 6], data hiding [7, 8], and watermarking [9, 10].

Traditional text encryption methods are often inadequate for securing digital images, especially color images, due to their unique characteristics [11]. Ensuring the reliability and security of image encryption is crucial for protecting sensitive information. Various approaches have been proposed, including chaos-based encryption [12, 13], S-Box-based encryption [14], and DNA-based encryption [15]. This research focuses on chaos-based color-image encryption. Chaotic systems are known for their sensitivity to initial conditions and ability to generate seemingly random sequences [16-18]. These properties make them well-suited for encrypting digital images [19-22].

Image encryption involves transforming an image into an unintelligible form using a secret key. This key is then used to decrypt the image and restore its original content. To ensure the security of the encryption process, it must adhere to the principles of permutation and diffusion [23]. Chaos-based encryption, pioneered by Fridrich [24], utilizes chaotic maps to generate random sequences that are used to rearrange the pixels of the image. This process, known as permutation, reduces the correlation between pixels. Diffusion, which involves changing the pixel values, further enhances security by making the encrypted image less predictable [24]. By combining permutation and diffusion, image encryption algorithms can achieve higher security.

Various chaos-based image encryption techniques have been developed. For example, Quan et al. proposed an encryption algorithm that utilizes chaotic maps with Markov properties [25]. Wang et al. designed a new encryption method based on complex Lorenz and Chen systems, following the principles of Shannon and Fridrich [26]. Ali et al. introduced a new hyper-chaotic map called 2D-HLCM, derived from logistic, Henon, and ICMIC maps, for image encryption [27].

Image encryption involves altering the pixel order and values. Sun et al. proposed a chaotic system using super multi-stable memristors for image encryption [28]. Ali and Ali presented a three-step encryption scheme: permutation using a chaotic map, pixel substitution using an S-box generated from the same map, and XOR operation for value modification [29]. Xiang and Liu introduced an improved logistic map for color image encryption [30]. Mondal and Mandal proposed a hybrid pseudorandom number generator combined with genetic operations for digital image encryption [31]. Bouteghrine et al. developed a 3D discrete-time chaotic system specifically

Qutaiba K. Abed, Waleed A. Mahmoud Al-Jawher. 2024, New Colorful Image Encryption Method Using Triple Chaotic Maps and Grey Wolf Optimization (GWO). *Journal port Science Research*, 7(3), pp.228-245. https://doi.org/10.36371/port.2024.3.11

designed for color image encryption [32]. Mou et al. combined image compression and encryption using a hyper-chaotic map to enhance security and reduce transmission and storage costs [33]. Singh and Bhatnagar [45] introduce a biometric-based medical image security framework. By merging biometric features with cryptographic methods, they aim to bolster the robustness and security of the encryption process. ElKamchouchi et al. [46] propose a bijective encryption system that leverages a hybrid chaotic map for diffusion and DNA operations for confusion. This approach seeks to achieve optimal security and efficiency. Wang et al. [47] present a chaotic image encryption algorithm utilizing random dynamic mixing. The algorithm employs a chaotic map to generate random permutations and substitutions, thereby increasing encryption complexity. Gao [48] Proposes an enhanced Henon map for encrypting color images. The algorithm capitalizes on the map's chaotic properties to create a secure and efficient encryption scheme. Hosny et al. [49] introduce a novel encryption method for color images using a fractional-order hyperchaotic system. This approach leverages the system's complex dynamics to enhance security. Alexan et al. [50] propose a color image encryption algorithm combining chaos and the KAA map. This approach offers high-level security and resistance to various attacks [51-53].

While chaos-based image encryption algorithms offer various advantages, they also have limitations. To be effective, an algorithm should have a large keyspace to prevent statistical attacks, be adaptable to different image sizes, and reduce correlations in the encrypted images [34]. To assess the security of chaos-based encryption schemes, numerous cryptanalysis studies have been conducted, providing valuable insights for improving their robustness [35-37].

Using a single map to encrypt three channels in the color image was not sufficient for security, especially when using the same key to encrypt the three channels. This way, the correlations between adjacent pixels could be broken as a first level. Thus, in this paper, the correlations are broken into two levels. In the first level, the correlations are broken between adjacent pixels in each channel. Since the encryption is performed for each channel using a different map and key, the correlations between the channels are also broken, representing the second level [54-68].

The contributions of this paper are outlined as follows: Introducing a new encryption technique for colored images. It uses the confusion and diffusion stages by combining triple chaotic maps, URUK, WAM, and Nahrain chaotic maps. The plain-image pixels in each channel are shuffled using a specific distribution of four keys created by the triple chaotic maps [69-82]. Furthermore, the remaining keys diffuse the scrambled channels pixels, resulting in entirely different encrypted channels. Based on the chaotic characteristics of the triple maps used, combining these maps is an ideal solution for image encryption. By using distinct maps for each color channel and separate keys for scrambling and diffusing, the algorithm effectively eliminates the interdependencies between neighboring pixels and among the RGB channels. The proposed method demonstrates exceptional resistance to statistical and differential attacks and offers a vast key space [83-112].

The remainder of the paper as follows: Section 2 URUK chaotic system. Section 3 WAM 3D Discrete Chaotic Map. Section 4 The Nahrain Chaotic Map (NCM), Section 5 Gray Wolf Optimization (GWO) [113-129]. Section 6 explains the Encryption process, section 7 describes the decryption process, section 8 Discusses experiential results and analysis, and Section 9 shows the

2. URUK Chaotic System

The Uruk chaotic system is a relatively new mathematical model that exhibits chaotic behavior. This means it's a system that's sensitive to initial conditions, and unpredictable in the long term. The system operates in four dimensions (often denoted as A, B, C, and D) and evolves in discrete steps rather than continuously. It exhibits intricate and unpredictable behavior over time, even with small changes in its starting conditions. Due to its complex and unpredictable nature, the Uruk system has potential applications in cryptography and image encryption. The unpredictable outputs can be used to scramble data, making it unreadable to unauthorized users.9

$$
\begin{gathered}
A_{(n+1)} = 1 - (A_n \times B_n \times C_n \times D_n) - A_n^2 - B_n^2 - a \times \tan(C_n^2) - D_n^2 \\
B_{(n+1)} = A_n - b \times \tan(C_n) \\
C_{(n+1)} = B_n - c \times \tan(C_n) \\
D_{(n+1)} = A_n - d \times D_n \\
\dots \ (1)
\end{gathered}
$$

A mathematical system tracks four elements (A, B, C, and D) that can behave unpredictably. Certain values (a, b, c, and d) influence this erratic behavior. The system's equations are tweaked with trigonometric functions and complex interactions to make its outputs even more random [38] [39].

3. WAM 3D Discrete Chaotic Map

S Low-dimensional chaotic maps, while simple to implement, often exhibit unexpected deviations from theoretical behavior. To address this, we introduce a novel 3D discrete chaotic map, termed WAM. Defined by the following equations:

$$X_{n+1} = 1 - a \times Xn \times Yn - Xn\text{^}2 - Yn\text{^}2 - b \times \sin(Zn\text{^}2)$$

$$Y_{n+1} = Xn \qquad (2)$$

$$Z_{n+1} = \pi - Yn - c \times \sin(Zn)$$

The WAM map incorporates control parameters (a, b, and c) and system variables (x, y, and z). The inclusion of trigonometric functions and nonlinear terms contributes to the map's randomness. Notably, the first equation includes four

Qutaiba K. Abed, Waleed A. Mahmoud Al-Jawher. 2024, New Colorful Image Encryption Method Using Triple Chaotic Maps and Grey Wolf Optimization (GWO). *Journal port Science Research*, 7(3), pp.228-245. https://doi.org/10.36371/port.2024.3.11

cross-product terms, and both the first and third equations incorporate sine functions. These characteristics make the WAM map particularly well-suited for encryption and secure communication applications [40].

4. The Nahrain Chaotic Map (NCM)

It is a 3D mathematical model that can generate chaotic patterns. It's controlled by parameters (a, b, and c) and involves three variables (Xn, Yn, Zn). NCM is sensitive to initial conditions, meaning small changes can lead to big differences in output. This makes it useful for cryptography. The system is defined as the following:

$$X_{n+1} = 1 - a\times Xn\times Yn - Xn^2 - Yn^2 - b\times Zn^2$$

$$Y_{n+1} = Xn \qquad (3)$$

$$Z_{n+1} = Yn - c\times Zn$$

The NCM-based encryption method scrambles pixel values and positions in an image, making it difficult to decrypt without the correct key. This key is derived from the initial conditions of the NCM. The encryption process is strong against various attacks due to the high level of confusion and diffusion it introduces [41].

5. Gray Wolf Optimization (GWO)

Gray Wolf Optimization is a meta-heuristic optimization algorithm that draws inspiration from the hunting behaviors of gray wolves. The algorithm is modeled after the social structure and hunting tactics observed in wolf packs.

Key Concepts in GWO:

- Social Hierarchy: Gray wolves have a strict social hierarchy, with alpha, beta, delta, and omega wolves.
- Hunting Behavior: The alpha wolves lead the pack in hunting, while the beta and delta wolves assist. The omega wolves follow.
- Encircling Prey: Wolves encircle their prey, gradually narrowing the circle to capture it.
- Hunting Phase: The wolves attack the prey collectively.

How GWO Works:

1. Initialization: A population of "wolves" (potential solutions) is randomly generated.
2. Leadership Selection: The most promising solution is designated as the alpha, the second-most promising as beta, and the third-best as delta.
3. Encircling Prey: The wolves' positions are adjusted based on the alpha, beta, and delta wolves, mimicking the encircling behavior
4. Hunting: The wolves collectively move towards the optimal solution in a coordinated manner.
5. Termination: The algorithm stops when a predefined stopping criterion is met (e.g., maximum number of iterations or sufficient convergence).

GWO has been successfully applied to various optimization problems, including image processing, engineering design, and feature selection. Its effectiveness lies in its simplicity, robustness, and ability to balance exploration and exploitation [42][43][44].

6. Encryption Process

Figure 1 shows the basic structure of our proposed encryption algorithm. This method has two main steps. First, pixel positions are shuffled using random sequences and a gray wolf optimization process. Second, pixel values in the RGB channels are mixed up using different random sequences from a chaotic map. The specific encryption steps are explained in more detail below.

1. Input color image size of (256 × 256) pixels.
2. Break down the color image into its three primary color components: red, green, and blue. Each component should be a square image measuring 256 by 256 pixels.
3. Generate the initial keys for the URUK chaotic map as follows
   a. Convert the color image into a grayscale image
   b. The image is fed into a hashing function called SHA512. This function digests the image data into a unique 512-bit string
   c. The 512-bit hash is divided into 64 groups of 8 bits each. Each group is essentially a number between 0 and 255 (represented in decimal).
   d. Four key values, X, Y, Z, and W, are calculated using the following mathematical equations that likely involve these 64 decimal numbers.

$$key_1 = \sum_{1}^{16} H_i \quad , \quad X = \frac{mode(key_1 \times 2^6, 99)}{100} \qquad (4)$$

$$key_2 = \sum_{17}^{32} H_i \quad , \quad Y = \frac{mode(key_2 \times 2^6, 99)}{100} \qquad (5)$$

$$key_3 = \sum_{33}^{48} H_i \quad , \quad Z = \frac{mode(key_3 \times 2^6, 99)}{100} \qquad (6)$$

$$key_4 = \sum_{49}^{64} H_i \quad , \quad W = \frac{mode(key_4 \times 2^6, 99)}{100} \qquad (7)$$

4. Applying URUK , WAM and Nahrain chaotic map to generate s, g, u, v, x, y vectors.

Qutaiba K. Abed, Waleed A. Mahmoud Al-Jawher. 2024, New Colorful Image Encryption Method Using Triple Chaotic Maps and Grey Wolf Optimization (GWO). *Journal port Science Research*, 7(3), pp.228-245. https://doi.org/10.36371/port.2024.3.11

5. Uses s, u and x vectors to scramble each channel separately to get scrambled channels (red, green and blue).
6. Uses g, v and y to apply diffusion process to each channel (red, green and blue).

Im= Xor ([red, green, blue] , [g, v, y]) (8)

7. Applying the GWO to shuffle the position of each channel as follows
   a. convert the channel to 1D dimension
   b. generate the population of wolves
   c. sort the position of each wolf and get the index
   d. shuffle the position of each channel based on the indexes of wolves depending on the following objective function

Min FC=Correlation (channel) …….. (9)

   e. Repeat this process for every iteration, calculating the pixel correlation each time. The goal is to find the image with the lowest correlation, which will be the final encrypted image.

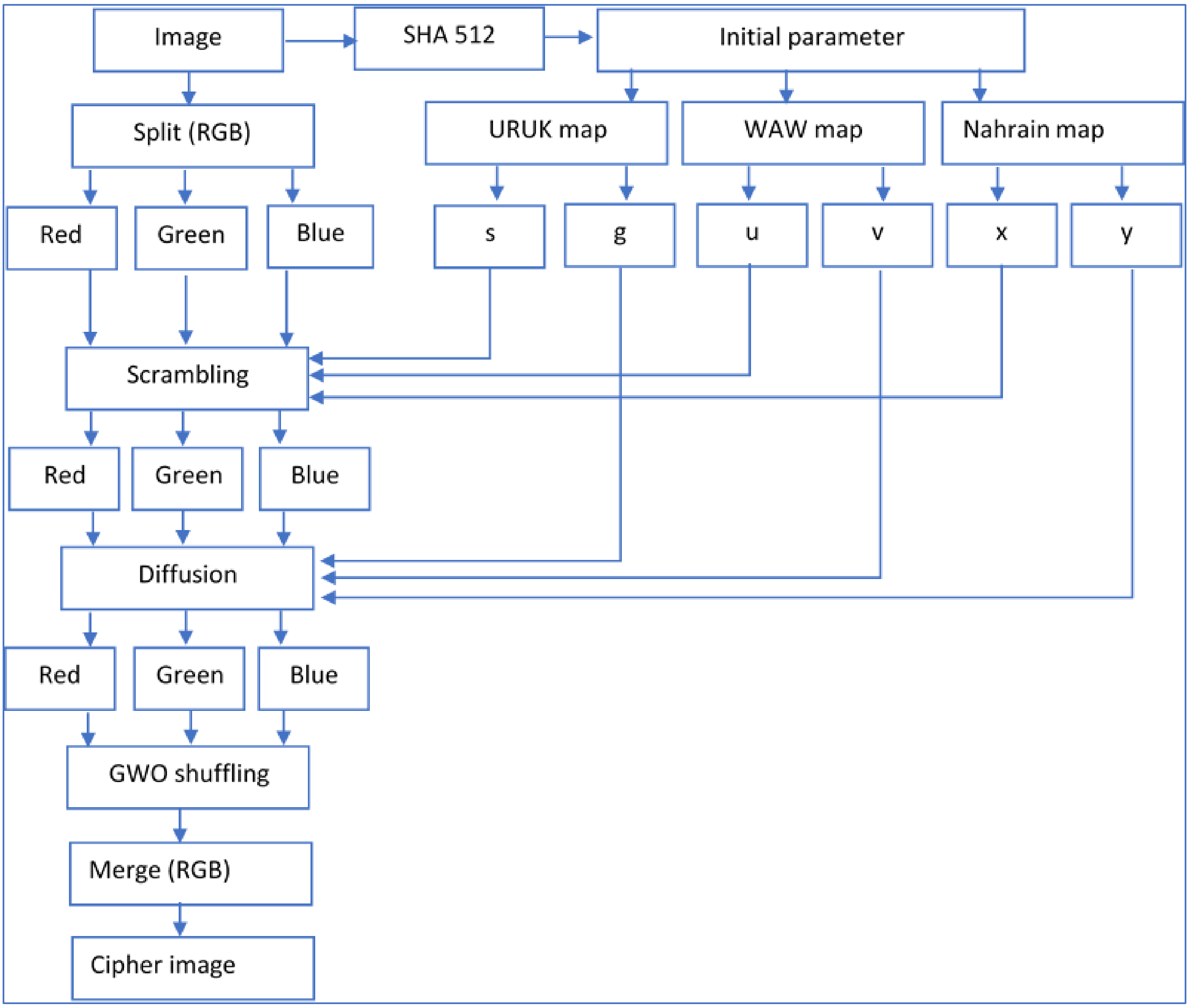


Figure 1: *block diagram for the proXposed encryption*

7. The Decryption Process

The decryption process is the inverse of the encryption process. The image is first divided into its individual color channels (red, green, and blue). For each channel, the pixel shuffling performed by the GWO algorithm during encryption is reversed. Next, the diffusion process is undone, returning the image to a partially scrambled state. Finally, the scrambling introduced by the triple chaotic sequence is reversed for each

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS
Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

channel, and the colors are recombined to recover the original plain image.

8. The Experiential Results And Analysis

Security analysis is a crucial step in evaluating the effectiveness of an encryption algorithm. It tests how well the algorithm can resist attacks that try to recover the original data from the encrypted version. This is particularly important for image encryption algorithms requiring specific security measures.

8.1 Keyspace analysis

Brute-force attacks are a common threat to encryption. To protect against them, we've designed our algorithm with a massive key space, far larger than the suggested minimum. This makes it nearly impossible for attackers to guess the correct key by trying every possibility.

Table 1. *Comparison of keyspace with different algorithms*

Algorithms	Proposed method	Ref. [45]	Ref. [46]	Ref. [47]
Key spaces	2^{199}	2^{99}	2^{213}	2^{186}

8.2 Information entropy

Information entropy is a measure of how unpredictable an image is. It shows how evenly the grayscale values are spread out in the image. A higher entropy means the image has more randomness or disorder [17]. The formula for calculating information entropy is as follows:

$$H(s) = -\sum_{i=1}^{L} p(x_i)\log_2 p(x_i), \qquad (10)$$

The formula for measuring information entropy includes the range of grayscale values (L) in an image and the probability (p(xi)) of each grayscale value appearing. For 8-bit grayscale images, the ideal entropy value is 8. Table 2 shows that encrypted images have entropy values close to 8, indicating high randomness. When compared to other algorithms using the Lena image, our algorithm achieves a higher entropy value, meaning the encrypted images are more random. This makes our algorithm less vulnerable to attacks that rely on statistical analysis.

Table 2: *calculation of entropy for the proposed method.*

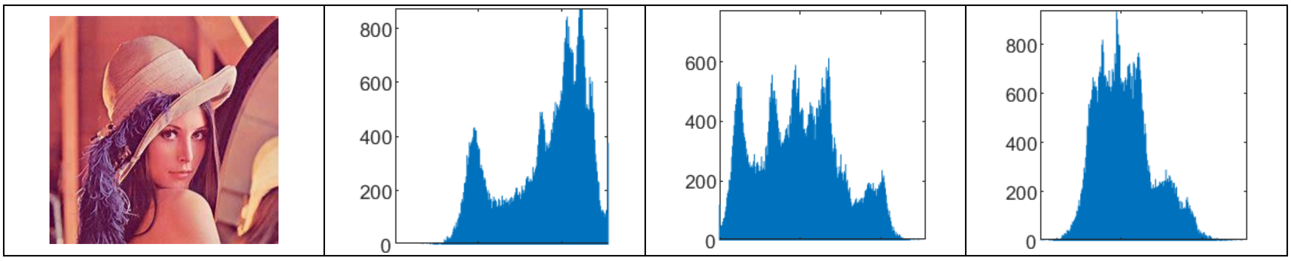
	Original			Cipher		
Image	R	G	B	R	G	B
Lena	7.3183	7.6042	7.1117	7.9975	7.9974	7.9972
Baboon	7.6058	7.3581	7.6665	7.9971	7.9973	7.9972
Pepper	7.3009	7.5570	7.0929	7.9974	7.9972	7.9976
Aircraft	6.7254	6.8253	6.2078	7.9974	7.9974	7.9972
Tree	7.2587	7.6143	7.1892	7.9969	7.9978	7.9967

Table 3: Comparison of entropy with other methods.

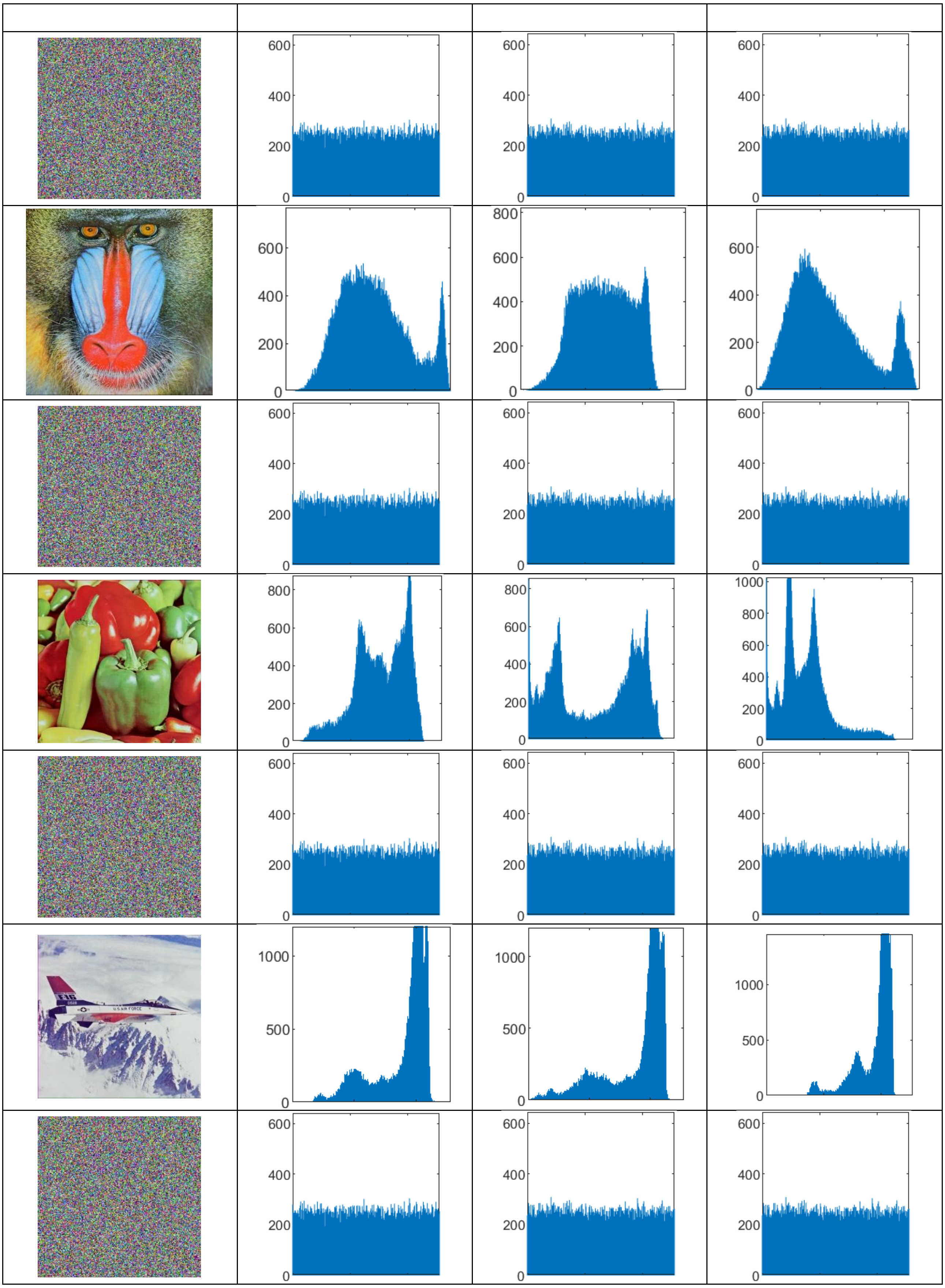
Method	R	G	B
Proposed method	7.9975	7.9974	7.9972
Ref [48]	7.9973	7.9972	7.9966
Ref [49]	7.9974	7.9971	7.9973
Ref [50]	7.9972	7.9965	7.9962

8.3. Histogram Analysis

An image histogram shows how pixel values are distributed in an image. If the histogram of an encrypted image is uniform, it means the original image information is well hidden. Figure 3 compares histograms of images before and after encryption. The flatter histograms of the encrypted images indicate that our algorithm effectively conceals the original image information and is less vulnerable to attacks that rely on statistical analysis.



Qutaiba K. Abed, Waleed A. Mahmoud Al-Jawher. 2024, New Colorful Image Encryption Method Using Triple Chaotic Maps and Grey Wolf Optimization (GWO). *Journal port Science Research*, 7(3), pp.228-245. https://doi.org/10.36371/port.2024.3.11



j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

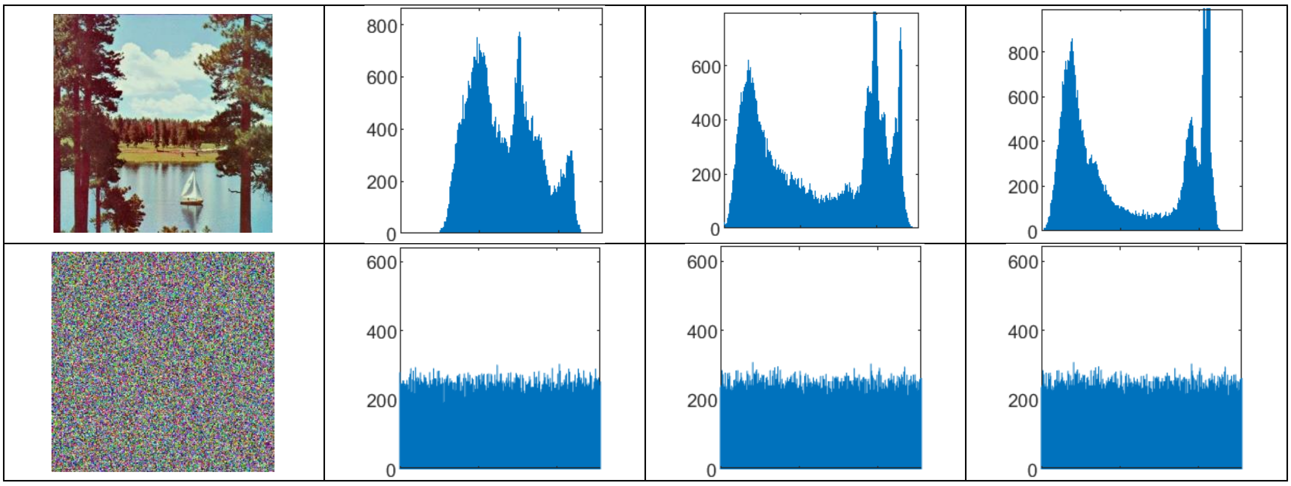


Figure 2: *Histogram analysis of colored images*

8.4 Correlation Analysis of Adjacent Pixels

Images with meaningful content have a strong connection between neighboring pixels. A good encryption algorithm should disrupt this connection to prevent attacks based on statistics. We examined how pixels are related in horizontal, vertical, and diagonal directions. Figure 4 shows that pixels in the original image are grouped, but in the encrypted image, they are spread out like noise. This indicates that the encryption algorithm has greatly reduced the correlation between pixels. To measure correlation numerically, we calculated the correlation coefficient using the following formula:

$$r_{i,j} = \frac{Co(i-Co(i)(j-Co(j)))}{\sqrt{D(i)D(j)}} \quad (11)$$

Table 4 presents the calculated correlation coefficients. As shown, the correlation coefficients of the encrypted images are significantly lower, approaching 0. Comparing our algorithm to others in Table 5, we find that our algorithm has lower correlation coefficients in all three directions (horizontal, vertical, and diagonal) for the Lena image. This means our algorithm can effectively break the relationship between neighboring pixels, making it more secure against statistical attacks.

Table 4: *Correlation of multiple cipher images.*

		Original			Cipher		
Image	direction	R	G	B	R	G	B
Lena	H	0.9399	0.9417	0.8886	0.0009	0.0000	0.0003
	V	0.9682	0.9697	0.9385	-0.0001	-0.0000	0.0000
	D	0.9086	0.9126	0.8352	0.0000	0.0011	0.0012
Baboon	H	0.9474	0.8728	0.9216	-0.0001	0.0000	-0.0009
	V	0.9208	0.8380	0.9139	0.0009	0.0001	-0.0003
	D	0.9034	0.7925	0.8763	-0.0000	0.0007	-0.0002
Pepper	H	0.9646	0.9698	0.9570	-0.0001	-0.0002	0.0004
	V	0.9680	0.9750	0.9636	0.0002	-0.0002	-0.0002
	D	0.9369	0.9466	0.9263	-0.0003	-0.0005	-0.0001
Aircraft	H	0.9389	0.9309	0.9503	0.0008	0.0005	0.0005
	V	0.9239	0.9343	0.9089	-0.0002	0.0001	-0.0010
	D	0.8738	0.8814	0.8800	-0.0003	-0.0002	-0.0000
Tree	H	0.9563	0.9558	0.9603	0.0002	-0.0001	-0.0002
	V	0.9539	0.9527	0.9645	0.0002	-0.0001	-0.0001
	D	0.9274	0.9225	0.9369	-0.0001	-0.0001	-0.0006

Table 5: *comparison of the Correlation of cipher colored-Lena.*

Method		R	G	B
Proposed	H	0.0009	0.0000	0.0003
	V	-0.0001	-0.0000	0.0000
	D	0.0000	0.0011	0.0012
Ref [48]	H	0.0007	−0.0035	0.0015

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS
Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

	V	−0.0004	0.0023	0.0028
	D	0.0039	−0.0079	−0.0010
Ref [49]	H	−0.0154	−0.0096	−0.0030
	V	−0.0102	0.0027	0.0117
	D	0.0159	−0.0162	−0.0026
Ref [50]	H	0.0073	−0.00054	0.00147
	V	−0.00508	0.00331	0.006219
	D	0.00311	0.00076	−0.00147

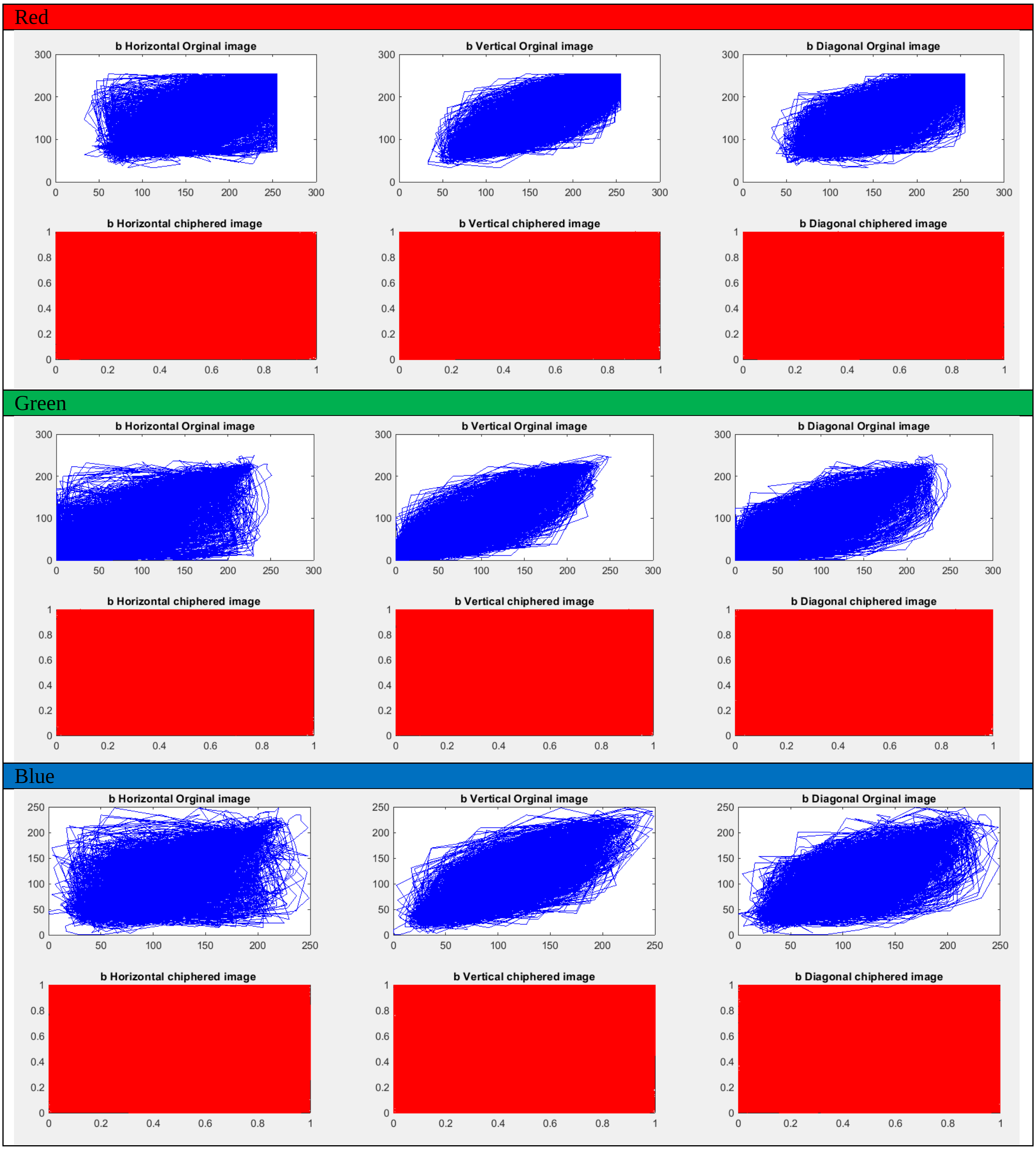


Figure 3: *The correlation of colored-Lena plain-image and corresponding ciphered-image*

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

8.5 Chosen/Known-Plaintext Attack Analysis

Chosen-plaintext and known-plaintext attacks are common security threats. Research indicates that an algorithm resistant to chosen plaintext attacks is also likely to be resistant to known plaintext attacks. Therefore, we focused on protecting against chosen-plaintext attacks. In our encryption algorithm, we use the SHA-512 hash of the plain image to generate the system parameters and initial values for the chaotic systems. This makes our algorithm very sensitive to changes in the plain image. If attackers try to encrypt slightly different images, they will get very different results. This prevents them from using special images to gather information. Additionally, we use bit-level XOR operations between different bit-planes. This makes it impossible for attackers to use special images to simplify the diffusion process.

8.6 Cropping Attack and Noise Attack Analysis

Images transmitted over networks can be vulnerable to data loss and corruption caused by noise. A robust image encryption algorithm should be able to safeguard against these threats, including cropping attacks. We tested our encryption algorithm on the "Lena" image and found that the decrypted image remains recognizable to humans even when portions of the encrypted image are cropped. This demonstrates the algorithm's resilience to cropping attacks. To assess the algorithm's resistance to noise, we introduced salt-and-pepper noise at varying levels (0.01, 0.03, 0.05, and 0.1) to the encrypted image. As depicted in Figure 6, while some noise is apparent in the decrypted images, the majority of the original image information remains discernible. This indicates that our algorithm is effective in mitigating noise attacks.

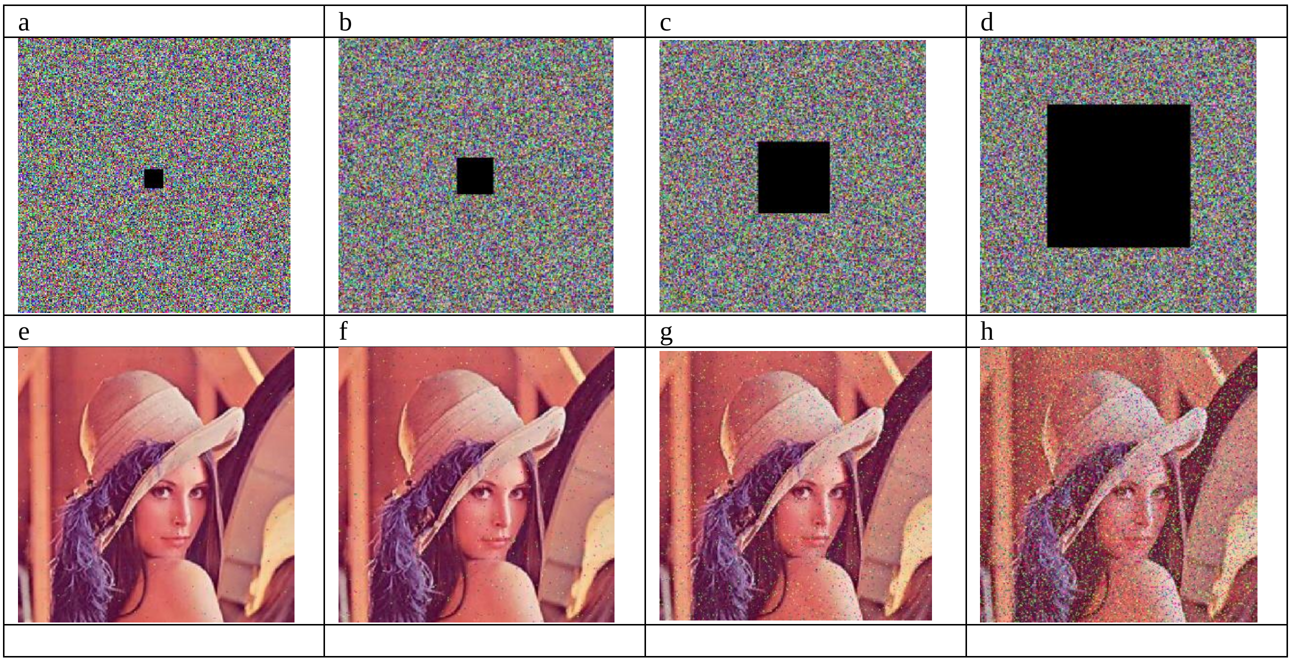
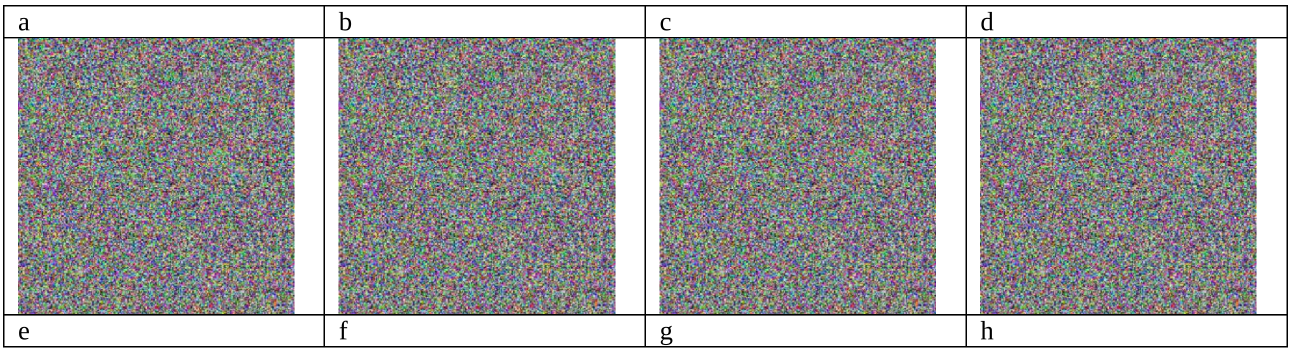


Figure 4. *The results of cropping attack, the encrypted images (a, b, c, d) with data loss of (16×16) pixels, (32×32) pixels, (64×64) pixels, (128×128), respectively where the images (e, f, g and h) are the decrypted images with PSNR (32.5897, 26.3571, 20.5842 and 14.5633) respectively*



j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

Figure 5 *illustrates the impact of noise attacks on an encrypted image. Panel (a) shows the encrypted image with a low level of salt and pepper noise (0.01), while panels (b), (c), and (d) display the image with progressively higher noise levels (0.03, 0.05, and 0.1, respectively).*
Panels (e) through (h) present the decrypted versions of the images corresponding to noise levels (a) through (d). The associated PSNR values (Peak Signal-to-Noise Ratio) are 30.7003, 25.8288, 23.7724, and 20.7223, respectively, indicating a gradual decline in image quality as the noise level increases.

8.7 MSE and PSNR

A coded image should look very different from the original. To measure this difference, we can use Mean Square Error (MSE). It can be calculated through:

$$\text{MSE}_{(P,E)} = \frac{1}{W\times H}\sum_{i=0}^{W}\sum_{j=0}^{H}\left(P(i,j) - E(i,j)\right)^2 \quad (12)$$

where $P(i, j)$ is the value of the pixels of the plain image and $E(i, j)$ is the encrypted pixel value at position (i, j) in the cipher image. The MSE value can serve as a criterion for assessing the encryption strength of a cryptosystem. The larger the MSE scale, the greater the encryption security.

PSNR is a way to measure encryption quality. A higher PSNR means the coded image is closer to the original. So, a lower PSNR indicates better encryption. We can calculate PSNR as follows:

$$\text{PSNR} = 20 \times \log_{10}[255/\sqrt{\text{MSE}}] \quad (13)$$

The MSE and PSNR values in Table 6 are between the plain image and the cipher image.

Table 6: *PSNR & MSE.*

	MSE			PSNR		
Image	R	G	B	R	G	B
Lena	169.0661	87.8112	94.8710	7.8618	8.5471	9.5219
Baboon	126.0315	117.9053	103.1464	8.9361	9.4974	8.5345
Pepper	139.7113	106.1949	56.9052	9.1320	7.6341	7.6874
Aircraft	167.3713	167.4557	179.3704	8.1737	7.8471	7.9783
Tree	119.8069	113.5575	104.4267	9.5069	7.5774	7.6074

8.8 Differential attack

Two standard methods, UACI and NPCR, are used to evaluate how well an encryption system can withstand a type of attack called a differential attack. These measures assess the extent of changes in the image after encryption.

$$\begin{cases} \text{UACI} = \frac{1}{w\times b} \times \sum_{x=0}^{w}\sum_{y=0}^{b}\frac{|C_1(x,y) - C_2(x,y)|}{255} \times 100\% \\ \text{NPCR} = \frac{1}{w\times b} \times \sum_{x=0}^{w}\sum_{y=0}^{b} D(x,y) \times 100\% \end{cases} \quad (14)$$

Where

$$D(x,y) = \begin{cases} 0, C_1(x,y) = C_2(x,y) \\ 1, C_1(x,y) \neq C_2(x,y) \end{cases} \quad (15)$$

Two encrypted images, C1 and C2, were created from plain images that differed by only one pixel. The UACI and NPCR values were calculated to evaluate how sensitive the encryption method is to small changes in the input. A strong encryption method should produce very different output images even if the input images are only slightly different. The results show that the method used in this study is resistant to differential attacks. It produces high NPCR values (close to 100%) and UACI values greater than 33%. This means that even a small change in the input image results in a big change in the encrypted image.

Qutaiba K. Abed, Waleed A. Mahmoud Al-Jawher. 2024, New Colorful Image Encryption Method Using Triple Chaotic Maps and Grey Wolf Optimization (GWO). *Journal port Science Research*, 7(3), pp.228-245. https://doi.org/10.36371/port.2024.3.11

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 7, issue 3. 2024

Table 7: *UACI and NPCR values for encrypted images.*

	UACI%			NPCR%		
Image	R	G	B	R	G	B
Lena	33.519	33.5247	33.5241	99.5605	99.5926	99.6231
Baboon	33.509	33.5787	33.4465	99.5895	99.6292	99.6231
Pepper	33.3802	33.3176	33.4242	99.6033	99.5605	99.6063
Aircraft	33.5433	33.5468	33.5728	99.6429	99.678	99.5605
Tree	33.4654	33.5622	33.4148	99.6353	99.5865	99.6521

Table 8: *Comparison of UACI and NPCR.*

	UACI%			NPCR%		
Image	R	G	B	R	G	B
Proposed	33.519	33.5247	33.5241	99.5605	99.5926	99.6231
Ref [48]	33.5031	33.4968	33.4515	99.6141	99.6101	99.6163
Ref [49]	33.4128	33.4980	33.4974	99.6017	99.6063	99.6368
Ref [50]	33.0704	30.7620	27.8720	99.6254	99.6254	99.6254

9. Conclusion

This paper introduces a novel image encryption algorithm that leverages the chaotic properties of multiple maps to ensure robust security. The algorithm introduces a high degree of confusion and diffusion by combining the URUK, WAM, and Nahrain chaotic maps. The method employs distinct chaotic maps for each color channel to further enhance security and separate keys for the scrambling and hiding processes. To minimize pixel correlation, the paper utilizes a grey wolf optimization (GWO) algorithm to rearrange the pixels within the image. This shuffling process effectively disrupts the patterns and dependencies between neighboring pixels. The proposed encryption scheme was rigorously evaluated using a comprehensive set of metrics, including histogram analysis, entropy, mean squared error (MSE), peak signal-to-noise ratio (PSNR), correlation coefficient, key space analysis, and differential attacks. The results unequivocally demonstrate the algorithm's resilience against a wide range of attacks and its superior security performance compared to existing methods.

REFERENCES

[1] Magdy, M., Hosny, K.M., Ghali, N.I., Ghoniemy, S.: Security of medical images for telemedicine: a systematic review. Multimedia Tools Appl. 81(18), 25101–25145 (2022)

[2] Hosny, K.M., Zaki, M.A., Lashin, N.A., Fouda, M.M., Hamza, H.M.: Multimedia security using encryption: a survey. IEEE Access 11, 63027–63056 (2023)

[3] Q. K. Abed and W. A. Mahmoud Al-Jawher, "An Image Encryption Method Based on Lorenz Chaotic Map and Hunter-Prey Optimization," J. Port Sci. Res., vol. 6, no. 4, pp. 332-343, 2023.

[4] Q. Kadhim and W. A. Mahmoud Al-Jawher, "A New Multiple-Chaos Image Encryption Algorithm Based on Block Compressive Sensing, Swin Transformer, and Wild Horse Optimization," Multidiscip. Sci. J., vol. 7, no. 1, pp. 2025012, 2024.

[5] Kaur, S., Singh, S., Kaur, M., et al.: Systematic review of computational image steganography approaches. Arch. Comput. Methods Eng. 29, 4775–4797 (2022)

[6] Eid, W.M., Alotaibi, S.S., Alqahtani, H.M., Saleh, S.Q.: Digital image steganalysis: current methodologies and future challenges. IEEE Access 10, 92321–92336 (2022)

[7] Abdel-Aziz, M.M., Hosny, K.M., Lashin, N.A.: Improved data hiding method for securing color images. Multimedia Tools Appl. 80, 12641–12670 (2021)

[8] Hassan, F.S., Gutub, A.: Improving data hiding within colour images using hue component of HSV colour space. CAAI Trans. Intell. Technol. 7(1), 56–68 (2022)

[9] Hosny, K.M., Darwish, M.M.: Robust color image watermarking using multiple fractional-order moments and chaotic map. Multimedia Tools Appl. 81(17), 24347–24375 (2022)

[10] Magdy, M., Ghali, N.I., Ghoniemy, S., Hosny, K.M.: Multiple zero watermarking of medical images for Internet of medical things. IEEE Access 10, 38821–38831 (2022)

[11] Talhaoui, M.Z., Wang, X.: A new fractional one-dimensional chaotic map and its application in high-speed image encryption. Inf. Sci. 550, 13–26 (2021)

[12] Q. K. Abed and W. A. Mahmoud Al-Jawher, "A Secure and Efficient Optimized Image Encryption Using Block Compressive Sensing and Logistic Map Method" Journal of Cyber Security and Mobility, vol. 13, no. 5, pp. 1-24, 2024.

[13] Q. K. Abed and Waleed. A. Mahmoud Al-Jawher, "Enhanced Hyperchaotic Image Encryption with CAW Transform and Sea-Lion Optimizer" Journal of Cyber Security and Mobility, vol. 13, no. 6, pp. 1-32, 2024.

[14] Ramakrishnan, B., et al.: Image encryption based on S-box generation constructed by using a chaotic autonomous snap system with only one equilibrium point. Multimedia Tools Appl. 83(8), 23509–23532 (2024)

[15] Wen, H., et al. Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography. Journal of King Saud University—Computer and Information Sciences, 36(1), 101871. (2024).

[16] Wang, X., Liu, P.: A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Trans. Circuits Syst. I: Regul. Pap. 69(3), 1291–1301 (2021)

[17] Abed, Q. K., & Al-Jawher, W. A. M. (2024). Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. Journal Port Science Research, 7(3), .219–236.

[18] Liu, X., et al.: Memcapacitor-coupled Chebyshev hyperchaotic map. Int. J. Bifurcation Chaos 32(12), 2250180 (2022)

[19] Xu, J., & Zhang, H. The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system. Visual Computing, 45(1), 123-134 (2022).

[20] Gao, X., et al.: An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. J. King Saud Univ.—Comput. Inf. Sci. 34(4), 1535–1551 (2022)

[21] Han, X., et al.: A new set of hyperchaotic maps based on modulation and coupling. Eur. Phys. J. Plus 137(4), 523 (2022)

[22] Q. Abed and Waleed A. Mahmoud Al-Jawher, "Image encrypted using circular map, block compressed sensing and hyper GWO-COOT optimization," International Journal of Intelligent Engineering & Systems, vol. 17, no. 5, 2024.

[23] Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. 28(4), 656–715 (1949)

[24] Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurcation Chaos 08(06), 1259–1284 (1998)

[25] Liu, Q., et al.: A novel image encryption algorithm based on chaos maps with Markov properties. Commun. Nonlinear Sci. Numer. Simul. 20(2), 506–515 (2015)

[26] Wang, L., Song, H., Liu, P.: A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt. Lasers Eng. 77, 118–125 (2016)

[27] Ali, D.S., Alwan, N.A., Al-Saidi, N.M.G.: Image encryption based on highly sensitive chaotic system. AIP Conf. Proc. 2183(1), 080007 (2019)

[28] Sun, J., et al.: A memristive chaotic system with hyper multistability and its application in image encryption. IEEE Access 8, 139289–139298 (2020)

[29] Ali, T.S., Ali, R.: A new chaos-based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools Appl. 79(27-28), 19853–19873 (2020)

[30] Xiang, H., Liu, L.: An improved digital logistic map and its application in image encryption. Multimedia Tools Appl. 79, 30329–30355 (2020)

[31] Mondal, B., Mandal, T.: A secure image encryption scheme based on genetic operations and a new hybrid pseudorandom number generator. Multimedia Tools Appl. 79(25-26), 17497–17520 (2020)

[32] Bouteghrine, B., Tanougast, C., Sadoudi, S.: Novel image encryption algorithm based on new 3-D chaos map. Multimedia Tools Appl. 80, 25583–25605 (2021)

[33] Mou, J., et al.: Image compression and encryption algorithm based on hyper-chaotic map. Mob. Netw. Appl. 26, 1849–1861 (2021)

[34] Qian, X., et al.: A novel color image encryption algorithm based on three dimensional chaotic maps and reconstruction techniques. IEEE Access 9, 61334–61345 (2021)

[35] Wen, H., & Lin, Y. Cryptanalyzing an image cipher using multiple chaos and DNA operations. Journal of King Saud University—Computer and Information Sciences, 35(7), 101612 (2023).

[36] Q. K. Abed and Waleed A. Mahmoud Al-Jawher, "A Robust Image Encryption Scheme Based on Block Compressive Sensing and Wavelet Transform," Int. J. Innov. Comput., vol. 13, no. 1-2, pp. 7-13, 2022.

[37] Q. K. Abed and Waleed A. Mahmoud Al-Jawher, "A New Architecture of Key Generation Using DWT for Image Encryption with Three Levels Arnold Transform Permutation," J. Port Sci. Res., vol. 5, no. 3, pp. 166-177, 2022..

[38] A. A. Abdul-Kareem and Waleed A. Mahmoud Al-Jawher, "A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet-Fourier Transforms," J. Cyber Secur. Mobility, pp. 435-464, 2023.

[39] A. A. Abdul-Kareem and W. A. Mahmoud Al-Jawher, “URUK 4D DISCRETE CHAOTIC MAP FOR SECURE COMMUNICATION APPLICATIONS,” Journal Port Science Research, vol. 5, no. 3, pp. 131–142, Oct. 2022.

[40] Abdul-Kareem, A. A., & Al-Jawher, Waleed A. Mahmoud Al-Jawher (2022). WAM 3D discrete chaotic map for secure communication applications. International Journal of Innovative Computing, 13(1-2), 45-5

[41] Abdul-Kareem, A. A., & Mahmoud Al-Jawher, W. A. (2024). An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain. *International Journal of Computers and Applications*, *46*(5), 324-337.

[42] Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey wolf optimizer. *Advances in engineering software*, *69*, 46-61

[43] Abdul-Kareem, A. A., & Mahmoud Al-Jawher, W. A. (2023). Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos. *Journal of Electronic Imaging*, *32*(4), 043038-043038.

[44] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher, “Image Encryption Algorithm Based on Arnold Transform and Chaos Theory in the Multi-wavelet Domain”, International Journal of Computers and Applications, Vol. 45, Issue 4, pp. 306-322, 2023.

[45] Singh, S.P.; Bhatnagar, G. A Novel Biometric Inspired Robust Security Framework for Medical Images. IEEE Trans. Knowl. Data Eng. **2021**, 33, 810–823.

[46] ElKamchouchi, D.H.; Mohamed, H.G.; Moussa, K.H. A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion. Entropy **2020**, 22, 180.

[47] Wang, X.; Chen, S.; Zhang, Y. A chaotic image encryption algorithm based on random dynamic mixing. Opt. Laser Technol. **2021**, 138, 106837.

[48] Gao, X.: A color image encryption algorithm based on an improved Hénon map. Phys. Scr. 96(6), 065203 (2021)

[49] Hosny, K.M., Kamal, S.T., Darwish, M.M.: Novel encryption for color images using fractional-order hyperchaotic system. J. Ambient Intell. Hum. Comput. 13, 973–988 (2022)

[50] Alexan, W., et al.: Color image encryption through chaos and KAA map. IEEE Access 11, 11541–11554 (2023)

[51] Zahraa A Hasan, Suha M Hadi, Waleed A Mahmoud, "Speech scrambler with multiwavelet, Arnold Transform and particle swarm optimization" Journal Pollack Periodica, Volume 18, Issue 3, Pages 125-131, 2023.

[52] W. A. Mahmoud Al-Jawher Zahraa A Hasan, Suha M. Hadi "Speech scrambling based on multiwavelet and Arnold transformations" Indonesian Journal of Electrical Engineering and Computer Science, Volume 30, Issue 2, Pages 927-935, 2023.

[53] W. A. Mahmoud Al-Jawher, Zahraa A Hasan, Suha M. Hadi," Time Domain Speech Scrambler Based on Particle Swarm Optimization" International Journal for Engineering and Information Sciences, Vol. 18, Issue 1, PP. 161-166, 2023.

[54] Afrah U Mosaa, Waleed A Mahmoud Al-Jawher "A proposed Hyper-Heuristic optimizer Nesting Grey Wolf Optimizer and COOT Algorithm for Multilevel Task" Journal Port Science Research, Vol. 6, PP. 310,317, 2023.

[55] WA Mahmoud, AI Abbas, NAS Alwan "Face Identification Using Back-Propagation Adaptive Multiwavelet" Journal of Engineering 18 (3), 2012.

[56] Rasha Ali Dihin, Waleed A Mahmoud Al-Jawher, Ebtesam N AlShemmary "Diabetic Retinopathy Image Classification Using Shift Window Transformer", International Journal of Innovative Computing, Vol. 13, Issue 1-2, PP. 23-29, 2022.

[57] Rasha Ali Dihin, Ebtesam AlShemmary and Waleed Al-Jawher "Diabetic Retinopathy Classification Using Swin Transformer with Multi Wavelet" Journal of Kufa for Mathematics and Computer, Vol. 10, Issue 2, PP. 167-172, 2023.

[58] AHM Al-Heladi, W. A. Mahmoud, HA Hali, AF Fadhel "Multispectral Image Fusion using Walidlet Transform" Advances in Modelling and Analysis B, Volume 52, Iss. 1-2, pp. 1-20, 2009.

[59] Maryam I Mousa Al-Khuzaay, Waleed A Mahmoud Al-Jawher, "New Proposed Mixed Transforms: CAW and FAW and Their Application in Medical Image Classification" International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 15-21, 2022.

[60] Waleed A Mahmoud, Afrah Loay Mohammed Rasheed "3D Image Denoising by Using 3D Multiwavelet" AL-Mustansiriya J. Sci, Vol. 21, Issue 7, PP. 106-136, 2010.

[61] Adnan HM Al-Helali, Hamza A Ali, Buthainah Al-Dulaimi, Dhia Alzubaydi, Walid A Mahmoud "Slantlet transform for multispectral image fusion" Journal of Computer Science, Vol.5, Issue 4, PP. 263-267, 2009.

[62] Waleed. A. Mahmoud & I.K. Ibraheem "Image Denoising Using Stationary Wavelet Transform" Signals, Inf. Patt. Proc. & Class. Vol. 46, Issue 4, Pages 1-18, 2003.

[63] Waleed Ameen Mahmoud-Al-Jawher "Computation of Wavelet and Multiwavelet Transforms using Fast FourierTransform" Journal Port Science Research, Vol. 4, Issue 2, PP. 111-117, 2021.

[64] Mutaz Abdulwahab and Hadeel Al-Taai Waleed Ameen Mahmoud "New Fast Method for Computing Wavelet Coefficients from 1D up to 3D" , proceedings of the 1st Int. Conference on Digital Communication and computer Application, Jordan, Pages 313-323, 2007.

[65] Waleed A Mahmoud, Ahmed S Hadi "Systolic Array for Realization of Discrete Wavelet Transform " Journal of Engineering, Vol. 13, Issue 2, PP. 1-9, 2007.

[66] W. A. Mahmoud Z Jalal & N. K. Wafi "A New Method of Computing Multi-wavelets Transform using Repeated Row Preprocessing." Al-Rafidain Engineering Journal, Vol. 12, Issue 2, PP. 21-31., 2004.

[67] W. A. Mahmoud & I. A Al-Akialy "A Tabulated Method of Computation Multiwavelet Transform" Al-Rafidain University College, Vol. 15, PP. 161-170, Iraq, 2004.

[68] W. A. Mahmoud & Z. J. M. Saleh " An Algorithm for Computing Multiwavelets &Inverse Transform Using an Over-Sampled Scheme of Pre& Post processing respectively" Engineering Journal, Vol. 10, Issue 2, PP. 270-288, 2004.

[69] Walid A Mahmoud, Majed E Alneby, Wael H Zayer "2D-multiwavelet transform 2D-two activation function wavelet network-based face recognition" J. Appl. Sci. Res, Vol. 6, Issue 6, PP. 1019-1028, 2010.

[70] Waleed A Mahmoud, Dheyaa J Kadhim "A Proposal Algorithm to Solve Delay Constraint Least Cost Optimization Problem" Journal of Engineering, Vol. 19, Iss 1, PP 155-160, 2013.

[71] H. Al-Taai, Waleed A. Mahmoud & M. Abdulwahab "New fast method for computing multiwavelet coefficients from 1D up to 3D" , Proc. 1st Int. Conference on Digital Comm. & Comp. App., Jordan, PP. 412-422, 2007.

[72] A H Kattoush, Waleed Ameen Mahmoud Al-Jawher, O Q Al-Thahab "A radon-multiwavelet based OFDM system design and simulation under different channel conditions" Journal of Wireless personal communications, Volume 71, Issue 2, Pages 857-871, 2013.

[73] Waleed A. Mahmoud Al-Jawher, T Abbas – "Feature combination and mapping using multiwavelet transform" IASJ, AL-Rafidain, Issue 19, Pages 13-34, 2006

[74] WA Mahmoud, AS Hadi, TM Jawad "Development of a 2-D Wavelet Transform based on Kronecker Product" - Al-Nahrain Journal of Science, Vol. 15, Issue 4, PP. 208-213, 2012

[75] Saleem MR Taha, Walid A Mahmood "New techniques for Daubechies wavelets and multiwavelets implementation using quantum computing " 2013, Journal Facta universitatis-series: Electronics and Energetics, Volume 26, Issue 2, Pages 145-156, 2013.

[76] WA Mahmoud, ZJM Saleh, NK Wafi "The Determination of Critical-Sampling Scheme of Preprocessing for Multiwavelets Decomposition as 1st and 2nd Orders of Approximation" Journal of Al-Khwarizmi Engineering Journal, Volume 1, Issue 1, Pages 26-37, 2005.

[77] Saadi Mohammed Saadi, Waleed Al-Jawher" Enhancing image authenticity: A new approach for binary fake image classification using DWT and swin transformer" Global Journal of Engineering and Technology Advances, Vol. 19, Issue 3, PP. 1-10, 2024.

[78] AHM Al-Helali, Waleed A. Mahmoud, HA Ali "A Fast personal palm print authentication Based on 3d-multi–Wavelet Transformation", TRANSNATIONAL JOURNAL OF SCIENCE AND TECHNOLOGY, Vol. 2, Issue 8, 2012.

[79] WA Mahmoud, MS Abdulwahab, HN Al-Taai: "The Determination of 3D Multiwavelet Transform" IJCCCE, vol. 2, issue 4, 2005.

[80] AHM Al-Helali, WA Mahmoud, HA Hali, AF Fadhel "Multispectral Image Fusion using Walidlet Transform" Advances in Modelling and Analysis B, Volume 52, Issue 1-2, pp. 1-20, 2009.

[82] W. A. Mahmoud, J J. Stephan and A. A. Razzak "Facial Expression Recognition Using Fast Walidlet Hybrid Transform" Journal port Science Research، Volume3, No:1, Pages 59-69 2020.

[83] Waleed A. Mahmud Al-Jawher, Dr. Talib M. Jawad Abbas Al-Talib, Salman R. Hamudi "Fingerprint Image Recognition Using Walidlet Transform" Australian Journal of Basic and Applied Sciences, Australia, 2012.

[84] Hamid M Hasan, Waleed A. Mahmoud Al- Jawher, Majid A Alwan "3-d face recognition using improved 3d mixed transform" Journal International Journal of Biometrics and Bioinformatics (IJBB), Volume 6, Issue 1, Pages 278-290, 2012.

[85] Waleed A Mahmoud, MR Shaker "3D Ear Print Authentication using 3D Radon Transform" proceeding of 2nd International Conference on Information & Communication Technologies, Pages 1052-1056, 2006.

[86] Waleed Ameen Mahmoud "A Smart Single Matrix Realization of Fast Walidlet Transform" Journal International Journal of Research and Reviews in Computer Science, Volume 2, Issue, 1, Pages 144-151, 2011.

[87] Waleed Ameen Mahmoud "A Smart Single Matrix Realization of Fast Walidlet Transform" Journal of Research and Reviews in Computer Science, Volume 2, Issue, 1, PP 144-151, 2011.

[88] W. A. Mahmoud, J J. Stephan and A. A. Razzak "Facial Expression Recognition Using Fast Walidlet Hybrid Transform" Journal port Science Research، Volume3, No:1, Pages 59-69 2020.

[89] Dihin, R. Al-Jawher, Waleed and Al-Shemmary "Implementation of The Swin Transformer and Its Application In Image Classification" Journal Port Science Research, vol. 6, Issue 4, PP. 318-331. 2023.

[90] Waleed A Mahmoud Al-Jawher, Shaimaa A Shaaban "K-Mean Based Hyper-Metaheuristic Grey Wolf and Cuckoo Search Optimizers for Automatic MRI Medical Image Clustering" Journal Port Science Research, Volume 7, Issue 3, Pages 109-120, 2024.

[91] Waleed A Mahmoud Al-Jawher, Sarah H Awad "A proposed brain tumor detection algorithm using Multi wavelet Transform (MWT)" Materials Today: Proceedings, Volume 65, Pages 2731-2737, 2022.

[92] Walid Amin Mahmoud, Raghad Aladdin Jassim "Image Denoising Using Hybrid Transforms" Engineering and Technology Journal, Vol. 25, Issue 5, PP. 669-682, 2007.

[93] Walid A Al-Jawher, Nada N Al-Ramahi, Mikhled. Alfaouri, "Image Identification And Labeling Using Hybrid Transformation And Neural Network" Neural Network World: International Journal on Neural and Mass - Parallel Computing and Information Systems; Prague, Vol. 17, Issue 4, PP. 377-395, 2007.

[94] W. A. Mahmoud & Ommama Razaq "Speech recognition using new structure for 3D neural network" University of Technology, 1st Computer Conference, PP. 161-171, 2010.

[97] Maryam I Mousa Al-Khuzaie, Waleed A Mahmoud Al-Jawher "Enhancing Brain Tumor Classification with a Novel Three-Dimensional Convolutional Neural Network (3D-CNN) Fusion Model" Journal Port Science Research, Volume 7, Issue, 3, Pages 254-267, 2024.

[98] Walid A.Mahmoud Rafah Abdul Hadi, Seham Ahmed Al-Musewy "Color Image Compression using Ridgelet Transform and Spilt Quantization Image Video" Journal of Techniques, Vollume 24, Issue 3, Pages 70-87, 2011.

[99] Raghad Aladdin Jassim, Walid Amin Mahmoud "Image Denoising Using Hybrid Transforms" Journal of Engineering and Technology, Volume 25, Issue 5, Pages 669-680, 2007.

[100] Rasha Ali Dihin, Ebtesam N. AlShemmary and Waleed A. Mahmoud Al-Jawher "Automated Binary Classification of Diabetic Retinopathy by SWIN Transformer" Journal of Al-Qadisiyah for computer science and mathematics (JQCM), Vol 15, Issue 1, PP. 169-178, 2023.

[101] Rasha Ali Dihin, Ebtesam N AlShemmary, Waleed AM Al-Jawher, "Wavelet-Attention Swin for Automatic Diabetic Retinopathy Classification" Baghdad Science Journal, 2024.

[102] Qutaiba Kadhim, Waleed Ameen Mahmoud Al-Jawher "A New Multiple-Chaos Image Encryption Algorithm Based on Block Compressive Sensing, Swin Transformer, and Wild Horse Optimization" Multidisciplinary Science Journal, Vol. 7, Issue 1, PP. 2025012-2025012, 2025.

[103] KN Kadhim, SMR Taha, WA Mahmoud "A new method for filtering and segmentation of the ECG signal", Proceedings of the Annual International Conference of the IEEE Engineering …, 1988.

[104] WA Mahmoud, MS Abdul-Wahab, AA Sabri "A New Algorithm for Reconstruction of Lost Blocks Using Discrete Wavelet Transform" Engineering and technology journal 24 (10), 2005.

[105] L R. Hussssein andJ. M. A. Al-Sammarie W. A. Mahmoud "Image Identification using Minimum Distance Classifier with Multi-Wavelet Transform" Journal of Advances in Modelling and Analysis B, Volume 46, Issue (5-6), pages 1-22, 2003.

[106] Walid Amin Al-Jawhar, Ayman M Mansour, Zakaria M Kuraz "Multi technique face recognition using PCA/ICA with wavelet and Optical Flow" 2008 5th International Multi-Conference on Systems, Signals and Devices, pages 1-6, 2008.

[107] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher " An image encryption algorithm using hybrid sea lion optimization and chaos theory in the hartley domain" International Journal of Computers and Applications, Vol. 46, Issue 5, PP. 324-337, 2024.

[108] Qutaiba K Abed, Waleed A Mahmoud Al-Jawher "Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm" Journal Port Science Research, Vol. 7, Issue 3, PP. 210-236, 2024.

[109] WAM Al-Jawher, SAA SHABAN "Clustering Of Medical Images Using Multiwavelet Transform And K-Means Algorithms" Journal Port Science Research 5 (1), 35-42, 2022.

[110] Maryam I Al-Khuzaie, Waleed A Mahmoud Al-Jawher "Enhancing Medical Image Classification: A Deep Learning Perspective with Multi Wavelet Transform" Journal Port Science Research, Vol. 6, Issue 4, PP. 365-373, 2023.

[111] SM Saadi, WAM Al-Jawher "Proposed Deepfake Detection Method Using Multiwavelet Transform" International Journal of Innovative Computing 13 (1-2), 61-66, 2022.

[112] A. H. Salman, W. A. Mahmoud Al-Jawher "A Hybrid Multiwavelet Transform with Grey Wolf Optimization Used for an Efficient Classification of Documents" International Journal of Innovative Computing 13 (1-2), 55-60, 2022.

[113] Lamyaa Fahem Katran, Ebtesam N AlShemmary, Waleed AM Al-Jawher "A Review of Transformer Networks in MRI Image Classification" Al-Furat Journal of Innovations in Electronics and Computer Engineering, PP. 148-162, 2024.

[114] Saadi Mohammed Saadi, Waleed Ameen Mahmoud Al-Jawher "Proposed Deepfake Detection Method Using Multiwavelet Transform" International Journal of Innovative Computing, Vol. 13, Issue 1-2, PP. 61-66, 2022.

[115] Walid Amin Al-Jawhar, Ayman M Mansour, Zakaria M Kuraz "Multi technique face recognition using PCA/ICA with wavelet and Optical Flow" 5th International Multi-Conference on Systems, Signals and Devices, PP. 1-6, 2008.

[116] Waleed Ameen Mahmoud Al-Jawher, A. Barsoum and Entather Mahos "Fuzzy Wavenet (FWN) classifier for medical images" Al-Khwarizmi Engineering Journal, Vol. 1, Issue 2, PP. 1-13, 2005.

[117] Saadi M Saadi and Waleed A Mahmoud Al-Jawher "Image Fake News Prediction Based on Random Forest and Gradient-boosting Methods" Journal Port Science Research, Vol. 6, Issue 4, PP. 357-364, 2023.

[118] Lamyaa Fahem Katran, Ebtesam N AlShemmary, Waleed Ameen Al Jawher "Deep Learning's Impact on MRI Image Analysis: A Comprehensive Survey" Texas Journal of Engineering and Technology, Vol. 25, PP. 63-80, 2023.

[119] Ahmed Hussein Salman, Waleed Ameen Mahmoud Al-Jawher "A Hybrid Multiwavelet Transform with Grey Wolf Optimization Used for an Efficient Classification of Documents" International Journal of Innovative Computing, Vol. 13, Issue 1-2, PP. 55-60, 2022.

[120] Shaymaa Abdulelah Shaban, Waleed A Mahmoud Al-Jawher "K-Means Clustering Algorithm for Medical Images" International Journal of Advances in Engineering and Management (IJAEM), Vol. 4, Issue 11, 2022.

[121] Sarah H Awad Waleed A Mahmoud Al-Jawher "Precise Classification of Brain Magnetic Resonance Imaging (MRIs) using Gray Wolf Optimization (GWO)" HSOA Journal of Brain & Neuroscience Research, Volume 6, Issue 1, Pages 100021, 2022.

[122] W. A. Mahmoud, Jane Jaleel Stephan and A. A. W. Razzak "Facial Expression Recognition from Video Sequence Using Self Organizing Feature Map" Journal port Science Research و TRANSACTION ON ENGINEERING, TECHNOLOGY AND THEIR APPLICATIONS, Vol. 4, Issue 2, 2021.

[123] Ammar A Sakran, Suha M Hadi, Waleed A Mahmoud Al-Jawher "Advancing DNA Signal Processing: Integrating Digital and Biological Nuances for Enhanced Identification of Coding Regions" Journal Port Science Research, Volume, 6, Issue 4, Pages 374-387, 2023.

[124] Abbas Al-Talib Waleed A. Mahmud Al-Jawher, A. M. Ibrahim, Talib M. Jawad "Image Reconstruction Using Multi-Activation Wavelet Network" Australian Journal of Applied Sciences: Computer Science, Vol. 6, 410-417, 2012.

[125] Walid A Mahmoud, Majed E Alneby, Wael H Zayer "Multiwavelet Transform And Multi-Dimension-Two Activation Function Wavelet Network Using For Person Identification" Iraqi Journal Of Computers, Communications, Control And Systems Engineering, Vol 11, Issue 1, 2011.

[126] A. Barsoum and Entather Mahos Waleed. A. .Mahmoud "Fuzzy Wavenet (FWN) classifier for medical images" Al-Khwarizmi Engineering Journal, Vol. 1, Issue 2, PP. 1-13, 2005.

[127] Waleed A Mahmoud, Ahmed S Hadi "Systolic Array for Realization of Discrete Wavelet Transform " Journal of Engineering, Vol. 13, Issue 2, PP. 1-9, 2007.

[128] Waleed A Mahmoud Al-Jawher & N. Al-Ramahi "Hybrid Transformation Based Automatic Image Identification and Labelling" DCCA 2007 1st international conference on Digital communication & computer applications, Jordan, Pages 704-717, 2007.

[129] W. A. Mahmoud & Z. Ragib "Face Recognition Using PCA and Optical Flow" Engineering Journal, Vol. 13, Issue 1, PP. 35-47, 2007.

[130] L R. Husssseín andJ. M. A. Al-Sammarie W. A. Mahmoud " Image Identification using Minimum Distance Classifier with Multi-Wavelet Transform" Advances in Modelling and Analysis B, Volume 46, Issue (5-6), Pages 1-22, 2003.