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

Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm

Qutaiba K. Abed[1] , 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 new image encryption algorithm based on the Arnold transform and URUK chaotic maps is proposed to deal with the issues of inadequate security and low encryption efficiency. Colored images consist of three linked channels used in the scheme. This method uses different keys to break the correlations between adjacent pixels in each channel. First, the plain image is split into RGB channels to encrypt each channel separately. Second, the Arnold transform performs pixel permutation, resulting in scrambled channels. third, the URUK chaotic maps generate three key vectors to perform pixel diffusion, resulting in diffused channels used as input for the following step. Finally, the GWO shuffles each channel independently, to get the minimum correlation between image pixels, which are then merged to obtain a cipher image. This method generates the cipher image with great unpredictability and security. The security is evaluated using various measures. The results demonstrated a high level of security attained by successfully encrypting colored images. Recent encryption algorithms are compared in terms of entropy, correlation coefficients, and attack robustness. The proposed method provided outstanding security and outperformed existing image encryption algorithms.

10.36371/port.2024.3.3

Keywords: *Arnold transform, GWO, Fnet, URUK chaotic map*

1. INTRODUCTION

The advancement of multimedia technologies and the rise of the internet have led to a significant increase in information transmission, particularly digital images. These images play a vital role in various fields like remote sensing, medicine, and military communication. However, they can also contain sensitive personal or confidential information. Unauthorized access to this critical information can cause problems for both individuals and countries that own it [1,2]. This highlights the importance of protecting sensitive information. Encryption [3,4], steganography [5,6], data hiding [7,8], and watermarking are some of the common methods used to secure digital images [9,10].

While many encryption techniques exist, traditional methods designed for text aren't ideal for digital images, especially color ones. This is because color images have unique properties like redundancy, strong correlations between pixels, and large file sizes [11]. To ensure secure image encryption, reliable and robust methods are crucial. Researchers have proposed various approaches using different technologies, such as chaos theory [12, 13], substitution boxes [14], and even DNA [15]. This study specifically explores the use of chaos-based encryption for color images. Chaos theory is particularly useful for image encryption because even tiny changes in a chaotic system can lead to vastly different outcomes [16–18]. Additionally, chaotic systems are excellent at evenly covering a space (ergodicity), have a predictable past (determinism), and generate seemingly random numbers (pseudo-randomness) – all qualities ideal for encryption [19–22].

Image encryption aims to scramble an image using a secret key, making it appear random and unreadable. The same key is then used to decrypt the image and recover the original content. Following principles established by Shannon's information theory, effective encryption relies on two key techniques: permutation and diffusion [23]. Fridrich was a pioneer in chaos-based image encryption. His approach used chaotic maps to scramble the order of pixels in an image, relying on the iterative values generated by these maps [24]. As Shannon suggested, most image encryption methods involve both permutation and diffusion. Permutation rearranges the positions of pixels without changing their values, effectively reducing the correlation between them. Diffusion then alters the actual pixel values, creating the final encrypted image (cipher image). Combining permutation and diffusion provides a higher level of security [25-32].

The field of chaos-based image encryption has seen a steady rise in proposed techniques. For example, Quan et al. developed an encryption algorithm that utilizes chaotic maps with specific statistical properties [33]. Similarly, Wang et al. built upon Shannon and Fridrich's principles by designing a

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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 encryption method using complex chaotic systems from Lorenz and Chen [34]. Another contribution came from Ali et al., who introduced a novel hyper-chaotic map named 2D-HLCM. This map combines elements from logistic, Henon, iterative infinite folding, and infinite collapse maps, and it finds application in image encryption [35]. As mentioned earlier, encryption relies on manipulating both the order and the values of pixels. Sun et al. presented a unique chaotic system using special memristors for image encryption [36]. Ali and Ali proposed a three-step method for color image encryption [37]. First, they use a chaotic map to shuffle the pixel order in the original image (permutation). Next, they substitute pixel values using a substitution box derived from the same chaotic map. Finally, they perform an XOR operation to alter the pixel values themselves. Xiang and Liu improved upon the logistic map, using their enhanced version in a new color image encryption scheme [38]. Mondal and Mandal introduced a novel method that combines a pseudorandom number generator with genetic algorithms for image encryption [39]. Bouteghrine et al. created a new 3D chaotic system specifically designed for color image encryption [40]. Mou et al. took an innovative approach by combining image compression with encryption using a hyper-chaotic map. This not only enhances security but also reduces storage and transmission costs [41].

Despite their practicality, most chaos-based image encryption algorithms have both strengths and weaknesses. An ideal color image encryption algorithm should possess several key features: a vast and complex key space to thwart statistical attacks, the ability to handle images of any size, and a significant reduction in the original image's pixel correlations. To evaluate the effectiveness of these algorithms and identify areas for improvement, numerous studies have explored methods to break them (cryptanalysis) [42–48]. This ongoing research helps to strengthen the security of chaos-based image encryption schemes. Previous methods using a single 1D chaotic map for all color channels (red, green, and blue) had security weaknesses, especially when encrypting multiple images with the same key. This approach made it vulnerable to attacks that exploit correlations between adjacent pixels. This paper proposes a novel encryption technique for color images. It achieves this through a two-step process known as confusion and diffusion. The contribution lies in its combination of techniques:

- URUK Chaotic Maps and Arnold Transform: These work together to disrupt the original image's structure. The Arnold transforms shuffles pixels within each color channel, while URUK keys (X, Y, Z) significantly alter the values in these shuffled channels, creating entirely different encrypted versions.
- Grey Wolf Optimization (GWO) Algorithm: This further enhances security by shuffling pixels across all three channels (red, green, and blue). This minimizes any remaining correlations and ensures a highly random encrypted image.

By exploiting the chaotic nature of URUK maps, GWO, and Arnold transforms, the proposed method effectively breaks down correlations between neighboring pixels and across RGB channels. This significantly improves security by making the encrypted image resistant to common attacks like statistical and differential analysis. Additionally, the vast keyspace provided by the combined elements strengthens the encryption process.

The remainder of the paper as follows: Section 2 URUK chaotic system. Section 3 presents the Fnet transformer. Section 4 Gray Wolf Optimization (GWO). Section 5 explains the Encryption process, section 6 describes the decryption process, section 7 Discusses experiential results and analysis, and Section 8 shows some conclusions.

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 X, Y, Z, and W) 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.

$$X_{(n+1)} = 1 - (X_n \times Y_n \times Z_n \times W_n) - X_n^2 - Y_n^2 - a \times \tan(Z_n^2) - W_n^2$$

$$\begin{aligned} Y_{(n+1)} &= X_n - b \times \tan(Z_n) \\ Z_{(n+1)} &= Y_n - c \times \tan(Z_n) \\ W_{(n+1)} &= X_n - d \times W_n \end{aligned} \quad (1)$$

A mathematical system tracks four elements (x, y, z, and w) 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 [49].

3. Fnet Transformer

FNet streamlines the Transformer architecture by removing the self-attention mechanism in each encoder layer. Instead, it utilizes a Discrete Wavelet Transform (DWT) mixing sublayer [50-73]. This sublayer applies a 2D DWT to the data, achieving similar results without the computational burden of attention [74,75].

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

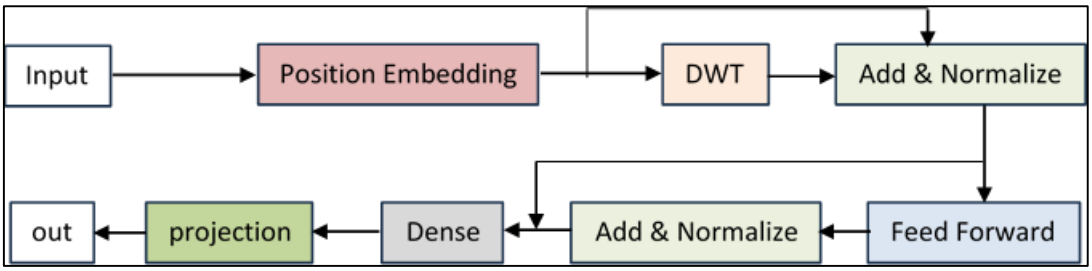


Figure 1: *FNet architecture with N encoder blocks.*

4. Gray Wolf Optimization (GWO)

GWO is a population-based optimization algorithm inspired by grey wolf social behavior during hunting.

- Social Hierarchy: It simulates a pack structure. Each candidate solution corresponds to a wolf. The "fittest" solution (one closest to the optimal value) is designated as the Alpha wolf. Beta and Delta wolves represent good solutions, while Omega represents the least fit.
- Hunting Phases: The optimization process mimics the hunting stages:
    1. Search: Wolves (solutions) update their positions based on the locations of Alpha, Beta, and Delta. This guides the search towards promising areas.
    2. Encircling Prey: Wolves strategically encircle the perceived prey (optimal solution) based on the positions of Alpha, Beta, and Delta.
    3. Attacking Prey: Wolves converge towards the prey to exploit it (find the optimal solution). This convergence process is mathematically modeled to iteratively improve solutions.
- Mathematical Modeling: The positions of wolves are represented by vectors, and their movements are controlled by mathematical equations that consider the social hierarchy and hunting behavior.

GWO offers a powerful tool for solving complex optimization problems in various fields like engineering design, machine learning, and scheduling [76-82].

5. Encryption Process

Figure 2 illustrates the primary structural diagram of our proposed algorithm. The proposed image encryption method consists of two stages: Confusion, where pixel positions are scrambled depending on the Arnold transform and gray wolf optimization algorithm. The second requires diffusion over the pixels of the RGB channels using Fnet and URUK chaotic map. The detailed encryption steps are described below:

1. Input color image size of (256 × 256) pixels.
2. separate the image (RGB format) into its individual red, green, and blue channels. Each of these channels with a size of 256 pixels by 256 pixels.
3. Applying Arnold transform to each channel separately to get scrambled channels
4. 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 scrambles 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.

$$key_1 = \sum_1^{16} H_i \quad , \quad X = \frac{mode(key_1 \times 2^6, 99)}{100} \qquad (2)$$

$$key_2 = \sum_{17}^{32} H_i \quad , \quad Y = \frac{mode(key_2 \times 2^6, 99)}{100} \qquad (3)$$

$$key_3 = \sum_{33}^{48} H_i \quad , \quad Z = \frac{mode(key_3 \times 2^6, 99)}{100} \qquad (4)$$

$$key_4 = \sum_{49}^{64} H_i \quad , \quad W = \frac{mode(key_4 \times 2^6, 99)}{100} \qquad (5)$$

5. Applying URUK chaotic map to generate X, Y, Z vectors and apply Fnet to each vector as follows
    a. Generate position encoding to each vector and add it to the original vector to get F vector
    b. Apply the DWT to the vector
    c. Apply a layer normalization to each vector to get F1 vector
    d. Add normalized vector F1 to the F vector to get F2
    e. apply multi-layer perceptron (MLP) for F2 vector to get F3.
    f. Apply a layer normalization to F3 vector to get F4 vector
    g. Add normalized vector F4 to the F3 vector to get F5 vector

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

h. apply the final multi-layer perceptron (MLP) for F5 vector to F6 vector.
i. Apply the following equation to F6 vector to get the final quantified vector between [0-255] which use in the diffusion process.

O=Round [mode (Y × 10^9, 256)]

6. Applying diffusion process to each channel using X, Y, Z vectors

Im=Xor ([red, green, blue] , [X, Y, Z]) (6)

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) (7)

continue for all iteration to get the minimum correlation between pixels to get the final cipher image

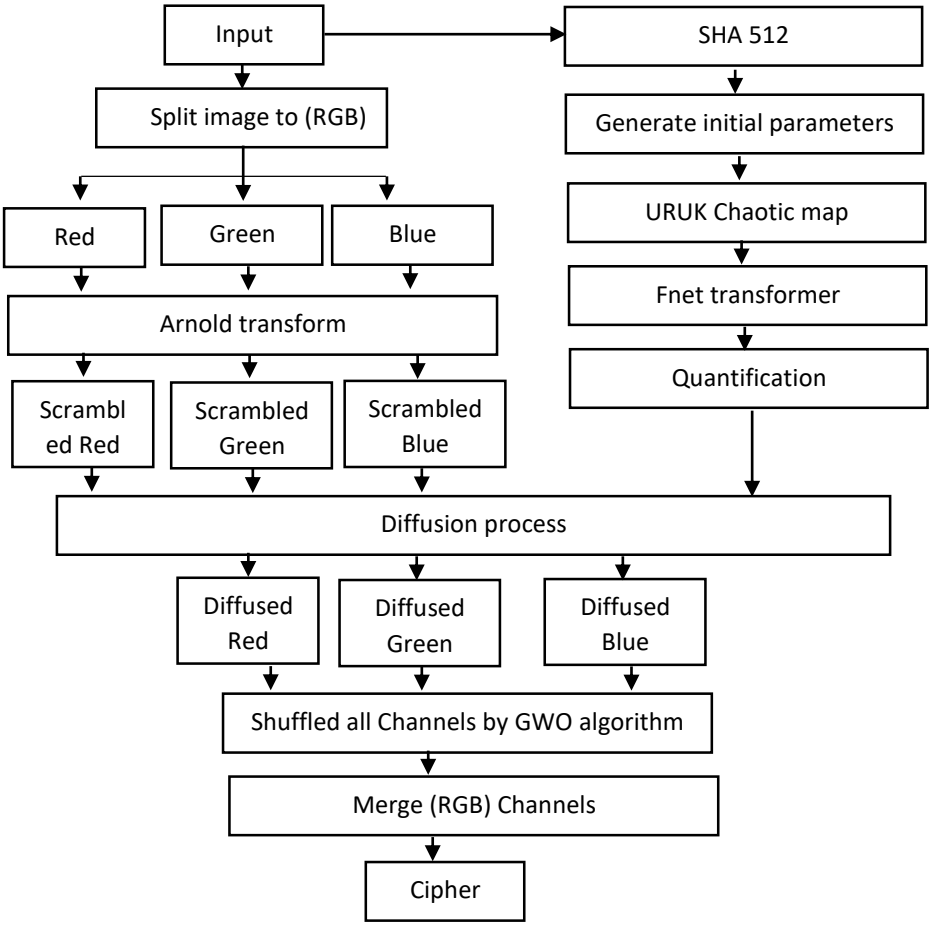


Figure 2: *block diagram for the proposed encryption*

6. The Decryption Process

The decryption process is the same as the encryption process, but in reverse. the image is divided into three channels (red, green and blue) where the shuffle of GWO is reversed for each channel. Next the diffusion process is reversed. finally, the scrambling is reversed by Arnold transform for each channel then colors are mixed to obtain the plain image.

7. The Experiential Results And Analysis

Security analysis is a crucial step to evaluate the performance of an encryption algorithm. It assesses how well the algorithm resists various attacks that aim to retrieve the original data from the encrypted ciphertext. Here is the common breakdown of security analysis for image encryption algorithms:

7.1 Keyspace analysis

Brute-force attacks are a major concern for encryption algorithms. To address this, we have designed our algorithm with a large key space, exceeding 2^100 (the recommended minimum size according to [46]). This vast number of possible keys, as shown in Table 1, makes our algorithm

highly resistant to brute-force attempts to crack the encryption.

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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 1. *Keyspace for different algorithms.*

Algorithms	proposed	Ref. [83]	Ref. [84]	Ref. [85]
Key spaces	2^{256}	2^{99}	2^{213}	2^{186}

7.2 Information entropy

Information entropy is an important indicator to describe the uncertainty of image information, which quantifies the distribution of the image's grayscale values [17]. Generally speaking, the higher the information entropy value, the higher the degree of disorder in the image. The formula of information entropy is as follows.

$$H(s) = -\sum_{i=1}^{L} p(x_i)\log_2 p(x_i), \qquad (8)$$

where L is the grayscale grade of the image, and p(xi) is the probability of the grayscale value xi.

For 8-bit noise type grayscale images, the ideal value of information entropy is 8. The information entropy of different plain images and their corresponding cipher images are listed in Table 2. As can be seen, values of the information entropy of all encrypted images are close to 8. Table 3 lists the comparison results with other algorithms for Lena. It is obvious that the proposed algorithm owns a larger information entropy compared with other algorithms, which means the cipher images encrypted by the proposed algorithm have a stronger randomness. Thus, the proposed algorithm can resist statistical attacks based on entropy.

Table 2: *Information entropy of the proposed method.*

	Original			Cipher		
Image	R	G	B	R	G	B
Lena	7.3183	7.6042	7.1117	7.9969	7.9968	7.9972
Baboon	7.6058	7.3581	7.6665	7.9973	7.9973	7.9974
Pepper	7.3009	7.5570	7.0929	7.9967	7.9972	7.9976
Aircraft	6.7254	6.8253	6.2078	7.9971	7.9974	7.9970
Tree	7.2587	7.6143	7.1892	7.9967	7.9975	7.9974

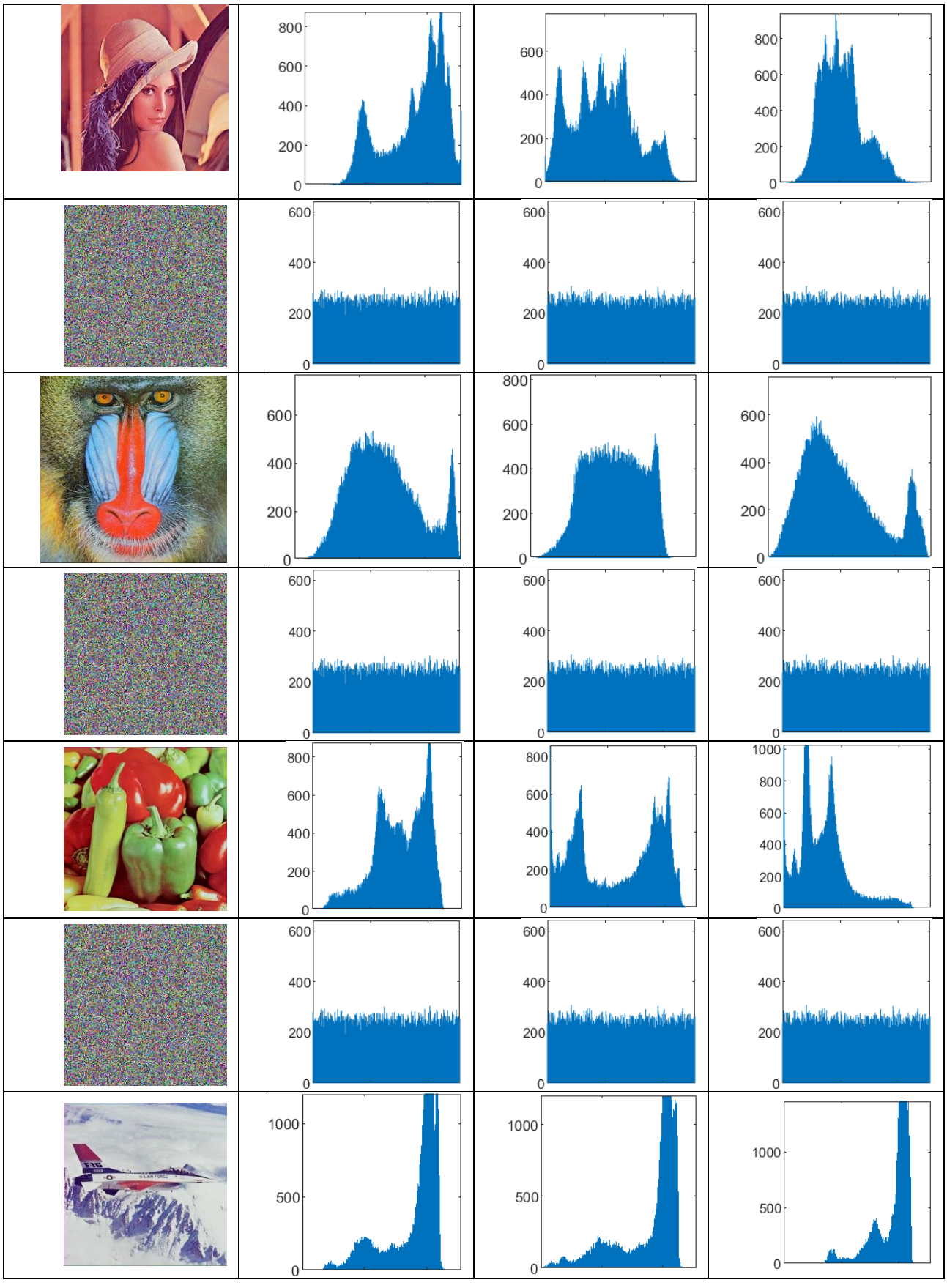
Table 3: Comparison of information entropy.

Method	R	G	B
Proposed	7.9969	7.9968	7.9972
Ref [86]	7.9973	7.9972	7.9966
Ref [87]	7.9974	7.9971	7.9973
Ref [88]	7.9972	7.9965	7.9962

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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



Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

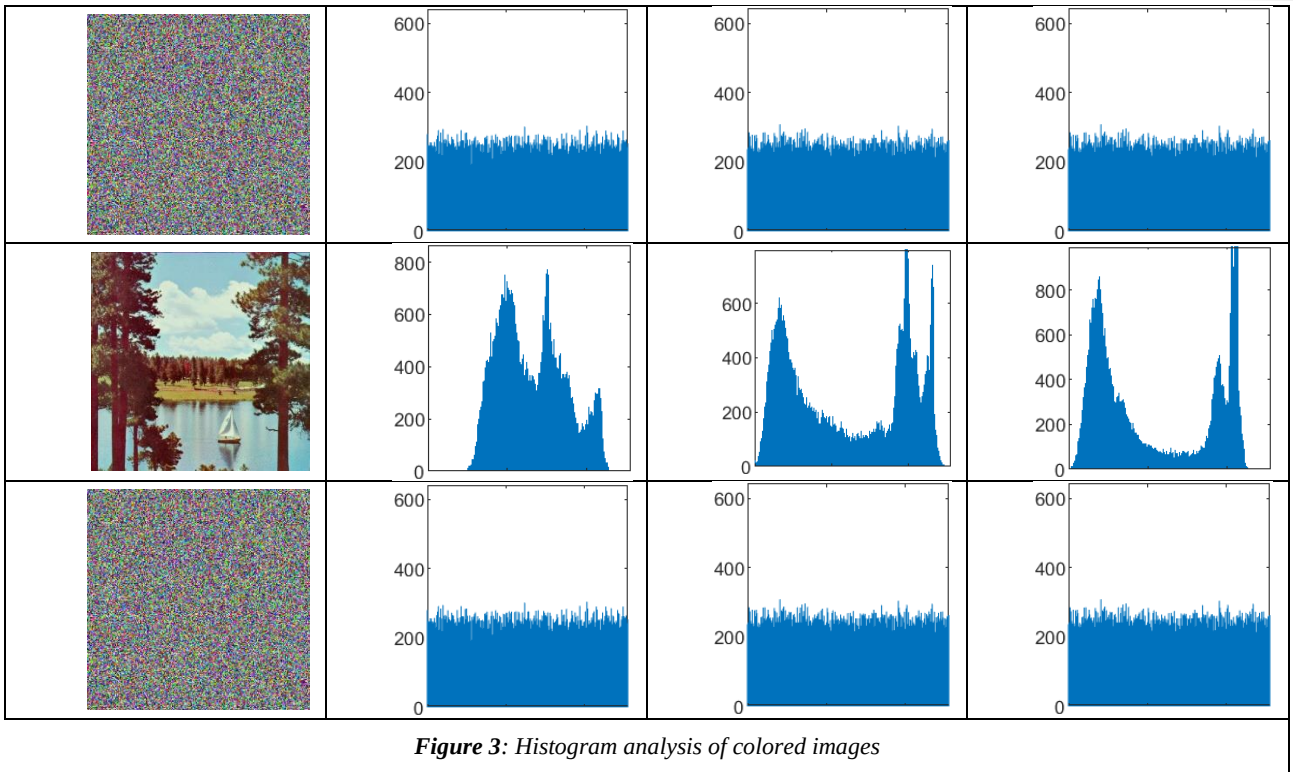


***Figure 3**: Histogram analysis of colored images*

7.3. Histogram Analysis

The distribution of image pixel values can be reflected by the image histogram. If the histogram of a cipher image is flat, information of the plain image is excellently hidden. Figure 3 shows the histograms of the images before and after encryption. It can be seen that the histograms of encrypted images become relatively flat. Therefore, the proposed algorithm can effectively resist statistical attacks.

7.4 Correlation Analysis of Adjacent Pixels

The plain image with effective information has a strong correlation between adjacent pixels. The ideal encryption algorithm can eliminate the correlation of adjacent pixels to resist statistical attacks. To ensure the reliability of the experiment of pixels are test the correlation in horizontal, vertical, and diagonal directions. As shown from Figure 4, the adjacent pixel distribution of the plain image is relatively concentrated, whereas the adjacent pixel distribution of the cipher image is noise-like. This means that the correlation of the plain image is greatly reduced. To quantitatively describe the correlation, the correlation coefficient is calculated as follows.

$$r_{i,j} = \frac{Co(i - Co(i)(j - Co(j)))}{\sqrt{D(i)D(j)}} \qquad (9)$$

The calculated correlation coefficients are shown in Table 4. It can be seen that the correlation coefficients of the cipher images have been greatly reduced, close to 0. The results compared with other algorithms as shown in Table 5. As can be seen, the correlation coefficients of Lena for the proposed algorithm are smaller in all three directions compared with other methods. The proposed algorithm can effectively remove the correlation of adjacent pixels, so it provides a high level of security to resist 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	0.0005	0.0013	-0.0005
	V	0.9682	0.9697	0.9385	-0.0003	0.0004	-0.0001
	D	0.9086	0.9126	0.8352	0.0004	0.0001	0.0000
Baboon	H	0.9474	0.8728	0.9216	0.0007	-0.0002	-0.0009
	V	0.9208	0.8380	0.9139	-0.0010	-0.0018	-0.0003

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

	D	0.9034	0.7925	0.8763	-0.0003	0.0005	-0.0003
Pepper	H	0.9646	0.9698	0.9570	0.0000	0.0001	0.0000
	V	0.9680	0.9750	0.9636	-0.0007	0.0005	-0.0012
	D	0.9369	0.9466	0.9263	-0.0001	-0.0008	0.0002
Aircraft	H	0.9389	0.9309	0.9503	0.0012	0.0009	0.0002
	V	0.9239	0.9343	0.9089	0.0010	0.0001	-0.0001
	D	0.8738	0.8814	0.8800	0.0001	-0.0012	0.0007
Tree	H	0.9563	0.9558	0.9603	0.0010	0.0002	0.0004
	V	0.9539	0.9527	0.9645	-0.0002	-0.0011	-0.0001
	D	0.9274	0.9225	0.9369	0.0007	0.0004	0.0001

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

Method		R	G	B
Proposed	H	0.0005	0.0013	-0.0005
	V	-0.0003	0.0004	-0.0001
	D	0.0004	0.0001	0.0000
Ref [86]	H	0.0007	−0.0035	0.0015
	V	−0.0004	0.0023	0.0028
	D	0.0039	−0.0079	−0.0010
Ref [87]	H	−0.0154	−0.0096	−0.0030
	V	−0.0102	0.0027	0.0117
	D	0.0159	−0.0162	−0.0026
Ref [88]	H	0.0073	−0.00054	0.00147
	V	−0.00508	0.00331	0.006219
	D	0.00311	0.00076	−0.00147

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

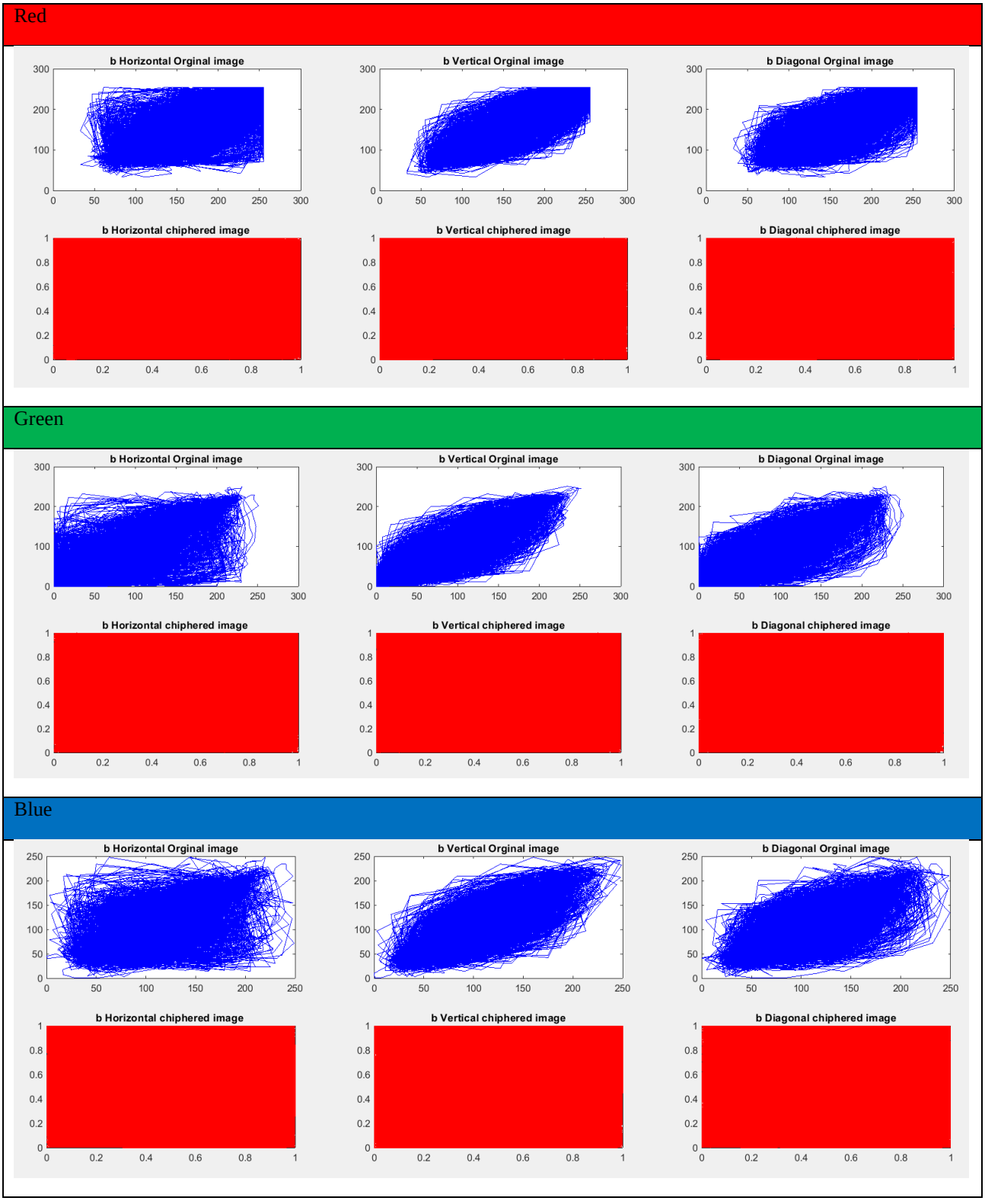


Figure 4: *The correlation of colored-Lena plain-image and corresponding ciphered-image*

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

7.5 Chosen/Known-Plaintext Attack Analysis

Chosen-plaintext and known-plaintext attacks are prevalent and high-threat types of attacks. The literature [59] indicated that an encryption algorithm with the capability to resist chosen-plaintext attacks can also resist known-plaintext attacks. Therefore, we only consider resisting chosen-plaintext attacks. Entropy In the proposed algorithm, we exploit the SHA-512 hash values of the plain image to generate the system parameters and initial values of the chaotic system, making the proposed algorithm highly sensitive to the plain image. Thus, when attackers use the proposed algorithm to encrypt slightly changed plain images, the encryption result obtained is totally different. Attackers cannot gain the desired information using special images. Furthermore, we perform bit-level exclusive-or operations between different bit-planes. Attackers are incapable of using special images to simplify the diffusion process.

7.6 Cropping Attack and Noise Attack Analysis

In the actual transmission process of the network, the images are at high risk of data loss or noise contamination. Therefore, a secure image encryption algorithm shall be robust against cropping attacks and noise. Take “Lena” as a test image. The cropped images are shown in Figure 5 a–h. We can see that even if cropping attacks on cipher images lead to data loss, the decrypted image can still be recognized by the human eye. This shows that the proposed algorithm is resistant to cropping attacks.

To test the anti-noise performance of the proposed algorithm, we add salt and pepper noise with different intensities to the cipher image, where the intensities are 0.01, 0.03, 0.05, and 0.1, respectively. The results are shown in Figure 6 a–h. It can be seen that the decrypted images contain some noises, but we can still recognize most of the information in the plain image by human eyes. The proposed algorithm is resistant to noise attacks. Thus, the proposed algorithm can effectively resist cropping attacks and noise attacks

.

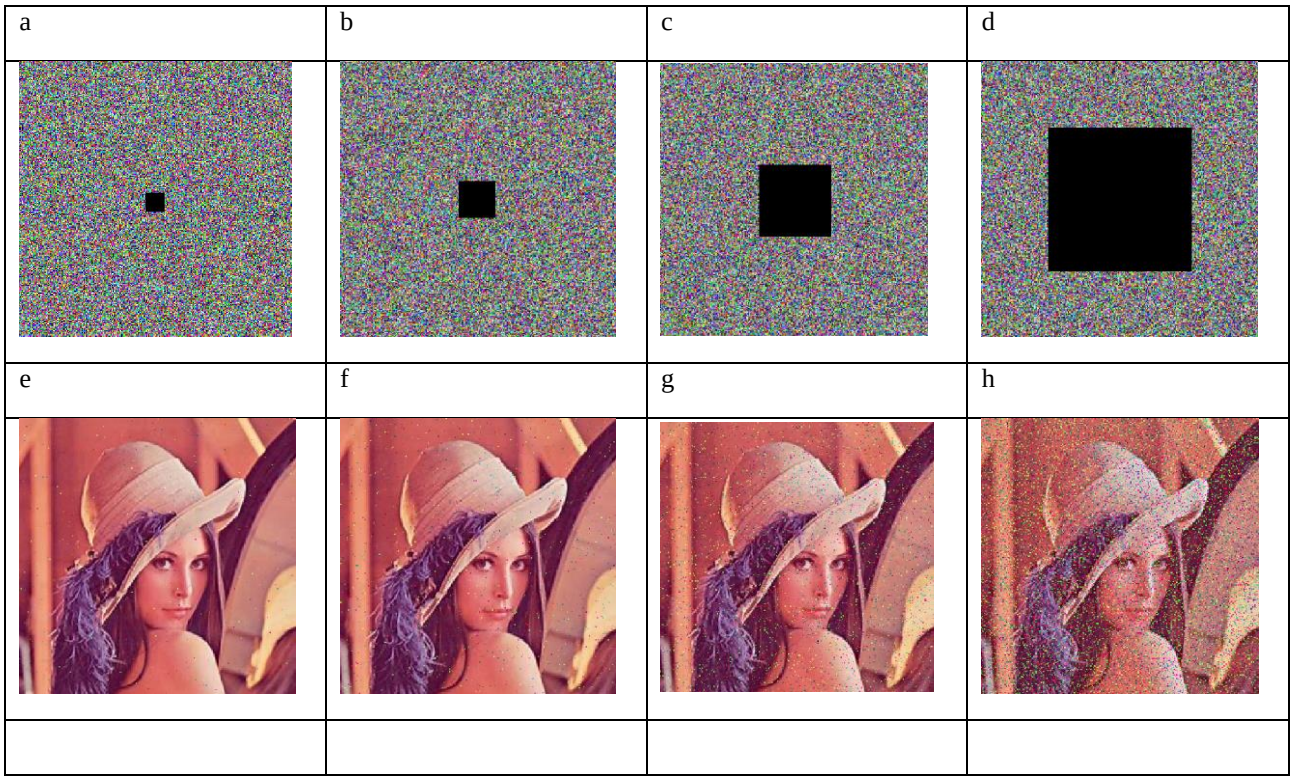


Figure 5. *The results of cropping attack, the encrypted images (a, b, c, d) with data loss of (16×16) pixels, (32×32) pixels, (64×64) pixels, (128×128), respectively where the images (e, f, g and h) are the decrypted images with PSNR (34.1651, 28.4776, 22.5790 and 16.6564) respectively*

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

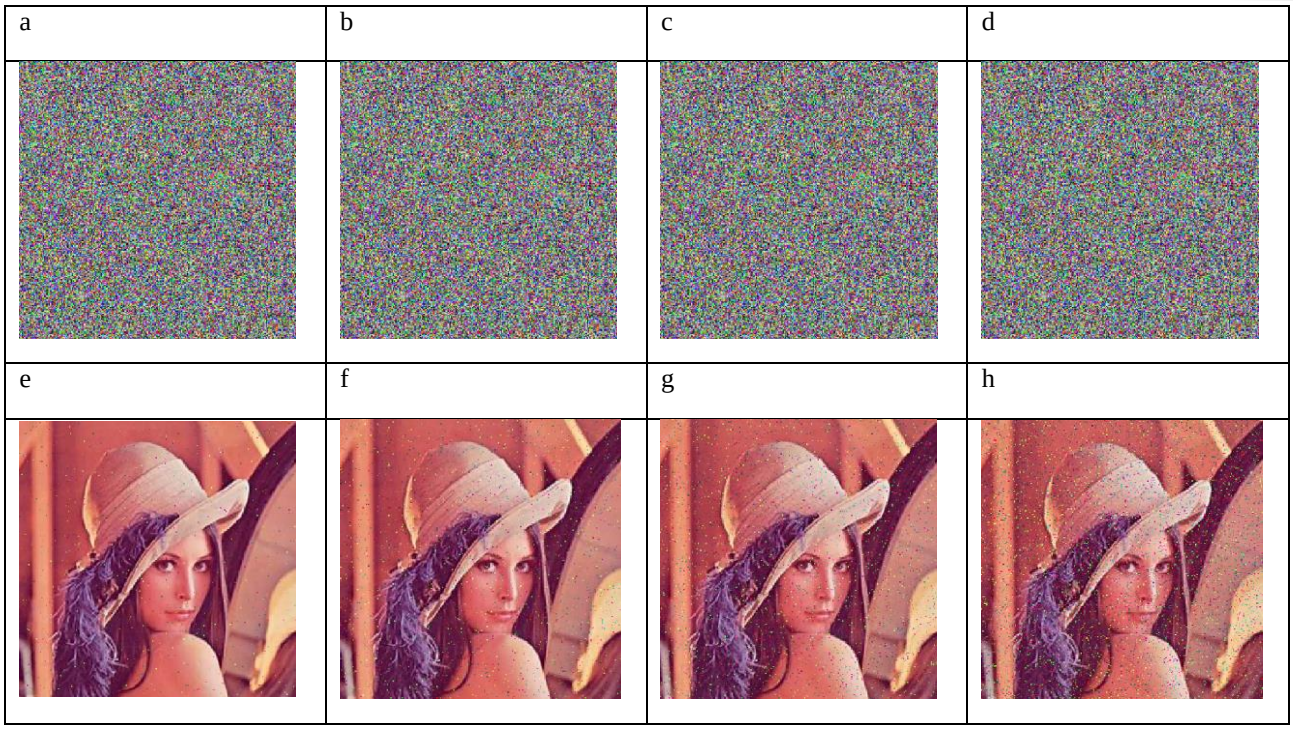


Figure 6. *The results of noise attack. (a) Encrypted image with 0.01 salt & pepper noise, (b) encrypted image with 0.03 salt & pepper noise, (c) encrypted image with 0.5 salt & pepper noise, (d) encrypted image with 0.1 salt & pepper, (e) decryption of (a) with PSNR=30.7003, (f) decryption of (b) with PSNR=25.8288, (g) decryption of (c) with PSNR=23.7724, and (h) decryption of (d) with PSNR=20.7223.*

7.7 MSE and PSNR

A ciphered image should exhibit substantial deviation from its original form. Mean square error (MSE) quantifies the cumulative squared difference between the original and corresponding ciphered images. It can be calculated through:

$$\mathrm{MSE}_{(P,E)} = \frac{1}{W \times H} \sum_{i=0}^{W} \sum_{j=0}^{H} (P(i,j) - E(i,j))^2 \qquad (9)$$

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 analysis is a way of deciding the encryption quality level; the higher the scale the closer the encrypted image is to the original image. Hence, a lower PSNR value indicates more robust encryption for a cryptosystem. It is calculated as follows:

$$\mathrm{PSNR} = 20 \times \log_{10}[255/\sqrt{\mathrm{MSE}}] \qquad (10)$$

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

Table 6: *PSNR & MSE.*

	MSE			PSNR		
Image	R	G	B	R	G	B
Lena	168.4700	88.3956	94.4988	7.8992	8.5331	9.5281
Baboon	126.3336	118.2624	102.7197	8.9241	9.4730	8.5792
Pepper	138.5282	106.0031	56.7380	9.1000	7.6646	7.6967
Aircraft	166.7014	166.9344	180.1188	8.1765	7.8837	7.9822
Tree	120.5613	114.3240	104.6394	9.5133	7.6103	7.5719

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

7.8 Differential attack

Two standard sensitivity measures are appointed to check the resisting level of the differential attack in this paper: unified average changing intensity (UACI) and the number of pixels change rate (NPCR). The definitions of UACI and NPCR are as follows:

$$\begin{cases} \text{UACI} = \frac{1}{w \times b} \times \sum_{x=0}^{w} \sum_{y=0}^{b} \frac{|C_1(x,y) - C_2(x,y)|}{255} \times 100\% \\ \text{NPCR} = \frac{1}{w \times b} \times \sum_{x=0}^{w} \sum_{y=0}^{b} D(x,y) \times 100\% \end{cases} \quad (11)$$

Where

$$D(x,y) = \begin{cases} 0, C_1(x,y) = C_2(x,y) \\ 1, C_1(x,y) \neq C_2(x,y) \end{cases} \quad (12)$$

The symbols $C1$,$C2$ refer to the two cipher images whose corresponding plain image has one random pixel variance, and (w,h) represents the number of rows and columns. In the 256 × 256 images, one pixel is selected randomly, and the pixel value is changed to value+1 and then encrypted. The calculated values of UACI and NPCR for different colored images are shown in Table 7. In addition, the values of UACI and NPCR of different algorithms are listed in Table 8. An encryption method is robust if a minor change in the algorithm's input results in a significantly different output; in other words, encrypting two nearly identical images exhibits an NPCR close to 100% and a UACI greater than 33%. The obtained results demonstrate that our method is robust against differential attacks.

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

	UACI%			NPCR%		
Image	R	G	B	R	G	B
Lena	33.5010	33.5307	33.5553	99.6368	99.6262	99.6338
Baboon	33.3539	33.4655	33.5937	99.5987	99.6170	99.6033
Pepper	33.4465	33.4444	33.5953	99.6094	99.6231	99.5850
Aircraft	33.4727	33.4271	33.4777	99.5789	99.6323	99.6704
Tree	33.6059	33.4008	33.5211	99.6384	99.6017	99.6170

Table 8: Comparison of UACI and NPCR.

	UACI%			NPCR%		
Image	R	G	B	R	G	B
Proposed	33.5010	33.5307	33.5553	99.6368	99.6262	99.6338
Ref [86]	33.5031	33.4968	33.4515	99.6141	99.6101	99.6163
Ref [87]	33.4128	33.4980	33.4974	99.6017	99.6063	99.6368
Ref [88]	33.0704	30.7620	27.8720	99.6254	99.6254	99.6254

8. CONCLUSION

In this paper, an image encryption technique is introduced. Its implementation involves the combination of URUK chaotic maps, Arnold transforms and GWO to introduce confusion and diffusion. Color separated into (red, green and blue) channel and a different key in each image is used for the confusion and diffusion processes. This process aided in breaking the correlation between neighboring pixels in each channel. The performance of the scheme was assessed using various measures. These comprised histogram, entropy, MSE, PSNR, correlation coefficient, key space and differential attack. The computed results indicate that the suggested technique is robust to all visual, statistical, differential, and brute-force attacks. Furthermore, the proposed image encryption technique provides comparable or greater security performance.

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

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] Tahiri, M.A., et al.: New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations. Vis. Comput. 39(12), 6395–6420 (2023)

[4] Hosny, K.M., Kamal, S.T., Darwish, M.M.: A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map. Vis. Comput. 39(3), 1027–1044 (2023)

[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] Wen, H., et al.: Chaos-based block permutation and dynamic sequence multiplexing for video encryption. Sci. Rep. 13(1), 14721 (2023)

[13] Wen, H., et al.: Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion. iScience 27(1), 108610 (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] Hosny, K.M., Kamal, S.T., Darwish, M.M.: Color image encryption technique using block scrambling and chaos. Multimedia Tools Appl. 81, 505–525 (2022)

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

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

[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] Ren, L., et al.: A hyperchaotic map with a new discrete memristor model: design, dynamical analysis, implementation, and application. Chaos, Solitons Fractals 167, 113024 (2023)

[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] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher ”Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos” , Journal of Electronic Imaging, Volume 32, Issue 4, Pages 043038-043038, 2023.

[26] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher, ”URUK 4D DISCRETE CHAOTIC MAP FOR SECURE COMMUNICATION APPLICATIONS” Journal Port Science Research, Vol. 5, Issue 3, PP. 131-141, 2023.

[27] 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, Volume 45, Issue 4, Pages 306-322, 2023.

[28] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher, “WAM 3D discrete chaotic map for secure communication applications” International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 45-54, 2022.

[29] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher” Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos” Journal of Electronic Imaging, Volume 32, Issue 4, Pages 043038-043038, 2023.

[30] 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.

[31] 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.

[32] 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.

Qutaiba K. Abed , Waleed A. Mahmoud Al-Jawher. 2024, Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm. *Journal port Science Research*, 7(3), pp.219-236. https://doi.org/10.36371/port.2024.3.3

[33] 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)

[34] 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)

[35] 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)

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

[37] 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)

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

[39] 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)

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

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

[42] 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)

[43] 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).

[44] Q. K. Abed and W. A. M. 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.

[45] Q. K. Abed and W. A. M. 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..

[46] Q. K. Abed and W. A. M. 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.

[47] Wen, H., Lin, Y., Feng, Z.: Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps. Eng. Sci. Technol. Int J. 51, 101634 (2024)

[48] Wen, H., Lin, Y.: Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Syst. Appl. 237, 121514 (2024)

[49] A. A. Abdul-Kareem and W. A. M. 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.

[50] 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.

[51] 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.

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

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

[54] WA Mahmoud, ALM Rasheed "3D Image Denoising by Using 3D Multiwavelet" AL-Mustansiriya J. Sci 21 (7), 108-136, 2010.

[55] [WA Mahmoud "Computation of Wavelet and Multiwavelet Transforms Using Fast Fourier Transform" Journal Port Science Research 4 (2), 111-117, 2021.

[56] 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 8, 1019-1028, 2010.

[57] 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.

[58] 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.

[59] AHM Al-Heladi, WA 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.

[60] 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.

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

[62] 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.

[63] 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.

[64] 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.

[65] WAM Al-Jawher, SH Awad "A proposed brain tumor detection algorithm using Multi wavelet Transform (MWT)" Materials Today: Proceedings 65, 2731-2737, 2022.

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

[67] 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.

[68] [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, Vol. 13, Issue 1-2, PP. 15-21, 2022.

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

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

[71] 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.

[72] 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.

[73] 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.

[74] J. Lee-Thorp, J. Ainslie, I. Eckstein, and S. Ontanon, "FNet: Mixing Tokens with Fourier Transforms," arXiv preprint arXiv:2105.03824, 2021.

[75] Q. Kadhim and W. A. M. 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.

[76] AH Salman, WAM 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.

[77] 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.

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

[79] 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.

[80] Ibraheem Al-Jadir, Waleed A Mahmoud "A grey wolf optimizer feature selection method and its effect on the performance of document classification problem" journal port science research, Vol. 4, Issue 2, Pages 125-131, 2021.

[81] Afrah U Mosaa, Waleed A Mahmoud Al-Jawher "A proposed Hyper-Heuristic optimizer Nesting Grey Wolf Optimizer and COOT Algorithm pages for Multilevel Task" Journal Port Science Research, Vol. 6, Issue 4, Pages 310-317, 2023.

[82] Afrah U Mosa, Waleed A Mahmoud Al-Jawher "Image Fusion Algorithm using Grey Wolf optimization with Shuffled Frog Leaping Algorithm" International Journal of Innovative Computing, Vol. 13, Issue 1-2, PP. 1-5. 2022.

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

[84] 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.

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

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

[87] 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)

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