2023, 20(6 Suppl.): 2593-2607
https://dx.doi.org/10.21123/bsj.2023.8715
P-ISSN: 2078-8665 - E-ISSN: 2411-7986

Baghdad Science Journal

Robust Color Image Encryption Scheme Based on RSA via DCT by Using an Advanced Logic Design Approach

Khalid Kadhim Jabbar *[1], ***Fahmi Ghozzi*** [2, 3], ***Ahmed Fakhfakh*** [2, 3]

[1]Department of Computer Science, Collage of Education, University of Mustansiriyah, Baghdad, Iraq.
[2]Departement of Electronic, National School of Electronics and Telecommunications of Sfax, University of Sfax, Sfax, Tunisia.
[3]Laboratory of signals, Systems, Artificial intelligence and Networks (SM@RTS), Digital Research Center of Sfax (CRNS),Sfax, Tunisia.
*Corresponding Author.

Received 08/03/2023, Revised 06/10/2023, Accepted 08/10/2023, Published 05/12/2023

Abstract

Information security in data storage and transmission is increasingly important. On the other hand, images are used in many procedures. Therefore, preventing unauthorized access to image data is crucial by encrypting images to protect sensitive data or privacy. The methods and algorithms for masking or encoding images vary from simple spatial-domain methods to frequency-domain methods, which are the most complex and reliable. In this paper, a new cryptographic system based on the random key generator hybridization methodology by taking advantage of the properties of Discrete Cosine Transform (DCT) to generate an indefinite set of random keys and taking advantage of the low-frequency region coefficients after the DCT stage to pass them to a subsystem consisting of an Reversible Logic Gate (RLG) group to obtain the secret keys that are passed to Rivest Shamir Adleman (RSA) to finish encrypting the image. The results indicate that the proposed method has the ability to generate a very large set of highly complex and secure secret keys that can be used later in the encryption stage. Moreover, the number and complexity of those keys will change each time the image is changed, and this represents the contribution of the proposed method. They experienced no time loss throughout the encryption and decryption processes when using RLG, which indicates that the proposed system did a good job in making different keys from the same image. And it differs in the strength of the key from one image to another, depending on the nature of the color imge.

Keywords: Cryptographic system, Decryption, DCT, Encryption, RLG, RSA.

Introduction

The importance of information security is based on the tremendous development in the field of communication and information exchange on the one hand, as well as the diversity in the sources of information that are transmitted through the internet environment, in which images play an effective role because of the ease of dealing with them.

The speed of sending them, and the high flexibility in their promotion and circulation among various circles. Given the sensitivity of these media because they contain important data, it has become necessary to provide means of protection for these images from intruders.

Security researchers have recently focused on protecting private images since unauthorized users routinely target uploaded data. Digital images have too much data, strong links between pixels, and redundant pixel values to be protected by text-based cryptographic algorithms as DES, AES, Twofish, RSA, Chaotic system, ...etc. For protection, images should be encrypted.[1-4]. To improve cryptosystem efficiency and security, several books and papers have been written about picture encryption approaches. This trade-off is unnecessary if a secure cryptosystem can be created without sacrificing speed.

Therefore, neither the general public nor cryptographers will accept it. To put it simply, a digital image is a collection of rectangles in two dimensions. Pixels are used to describe the individual components of this array. Each pixel is both a digital number representing its intensity and a physical address (row, column). In recent years, numerous strategies for protecting image data have been proposed. One of these useful shared resources is encryption. The algorithm used to combine the plain image with one or more keys throughout the encryption process is what ultimately produces the cipher image. Private Key techniques are a subset of ciphering methods in which the same key is used for both encryption and decryption. Asymmetric key approaches, on the other hand, encrypt using a public key and decrypt using a private key[5-7].

The reversible method has become well-known in recent years because it uses little power. Any time data is lost, vitality is also lost. Once an input can no longer be reconstructed from its output, the information it contained is gone forever. To solve the issue of low power consumption, reversible logic gates are used. A reversible system is a model in which the operations can be reversed, at least in part, over time. Reversibility can be broken down into two main categories: logical and physical. There is a direct mapping between input and output in reversible cryptographic logic designs. As a result, no savings in either energy or data are experienced. The number of reversible logic gates is a primary optimization element in reversible cryptographic logic[8].

On the other hand, with the availability of great facilities in the services that are provided by the World Wide Web to its users, which encouraged everyone from different companies and institutions to rely on that network to receive or provide services, and due to the expansion and development of that complex environment, the privacy of important and sensitive information has become more vulnerable to intruders. This matter has become a source of great concern for those interested, and they call for the provision of a mechanism to maintain the security aspect at various levels to ensure the continuity of these services.

Since then, experts have made numerous attempts to develop specialized technologies in this area, and encryption is one of those techniques. Encryption transforms stored data into intricate formats that require opening the code in order to understand. On the other hand, the degree of complexity and execution time is an important criterion in evaluating the proposed method of encryption, and based on these requirements, the current research aims to increase the complexity by generating non-repeatable secret keys.

The time factor, it used RLG, which is known for its high ability to reduce time as well as resource consumption, which increases the speed of implementation. Our proposed method aimed to present an effective method for designing reversible logic circuits based on color image texture by utilizing the properties of DCT for use in cryptography, taking into account such f actors as trash output, quantum cost, and delay time.

The rest of our paper is organized as follows: The relevant work paragraph, as for the most important tools that were used in building the proposed system, was clarified in the research methodology (RLG, XOR, RSA, and DCT).

As was the exact description of the proposed method, including algorithms, shapes, and related scheme including algorithms, shapes, and related schemes. At the stage of extracting facts about the success of the proposed method, this was presented in the results section. For more details, it shed light on the obtained results, but in a more detailed manner, in the discussion and analysis section. In the end, it was a review of the most important points reached in the conclusion paragraph.

Related Work

Many academics have come up with lightweight algorithms for cryptography that meet the needs of applications with limited time, space, and computing power. This section gives a summary of the most important things that lightweight algorithms have done so far.[9] Shows the RC7-RLGC algorithm, which is a way to use reversible logic gate complement (RLGC) to implement

Rivet's Cipher 7 (RC7) method for FPGAs. The pseudo-random numbers that are used as the encryption key are made by reversible logic gate circuits (RLGCs). This lets computers make good use of their resources. In[10], the idea of Reversible Logic Gates Cryptography Design (RLGCD) is explained. RLGCD is used to make both ciphers and ways to break them. With the help of a linear feedback shift register (LFSR), both the encryption and decryption keys are generated. For watermarking, the Least Significant Bit (LSB) technique is used to make the data safer. XTEA (extended TEA) has been called one of the most effective and efficient block ciphers in use today[11]. It has a compact code size, a lower memory requirement, and less processing power, and it works with simple addition, XOR, and shift functions. Even though the offered methods are good enough for reliability, the XTEA method is not as accurate in terms of error rate, which is a drawback. The Data Encryption Standard (DES) security component architecture using RLG is shown in[12], and it consists of a two-way shift register and a four-bit counter built on reversible logic gates. Using RLG to implement the security features of DES makes this task both quick and safe when it comes to protecting sensitive information. However, neither a specific RLG design nor any evaluations of its effectiveness are supplied.

Z. HA et al[13] changed the size of the S-box as well as the number of records that are needed to operate quickly in order to keep up with changing security threats. As a result of this study, a four-step matrix transformation has messed up the underlying structure of data blocks. This makes the cipher text safer than it was before. Then; cyclic byte displacement and the column ambiguity function were used to make the cipher-text diffusive. LFSR is then utilized to create dynamic effects. Thus, the secret key's stochastic feature is enhanced with each iteration; extreme scalability was attained using this method. However, the S-box is more challenging to achieve and takes more time to encrypt and decrypt when the selected dimension is an odd integer. In[14], two block ciphers were noticed; HIGHT and LED. While the former can be utilized in authenticated encryption techniques, the latter has a Feistel network structure and is better suited for low-power and low-complexity embedded applications. With regard to the latter, it employs the reliable Advanced Encryption Standard (AES) kind of encryption. Both the efficiency and error coverage of this approach are excellent. However, it cannot identify either permanent or temporary problems. [15]Symmetric decipherment and decryption are achieved by utilizing a key generated by a linear feedback shift register (LFSR) to counteract reversible logic cryptography (RLC). These advantages will add more complexity; moreover, some of the tools that will be dealt with will greatly reduce the time factor which will be shown in detail in the proposed method paragraph.

Statement of the Problem

The proposed method is distinguished from its counterparts from the previous methods by its ability to generate different and non-repeating secret keys because it depends in the basis of its work on the color nature of the image, and as everyone knows, the images vary in their color nature and differ from one image to another, and this in itself is considered a new contribution to this, in addition; transactions that are picked from the low-frequency region after the DCT stage are passed to a hybrid subsystem consisting of a set of RLG logic gates that generate those secret keys and then pass them to RSA to complete the encryption process, a new work methodology in this field.

Research Methodology

The scientific methodology of the current research depends on a set of tools that collected in one system to work in a coordinated manner, each according to its importance, to form an integrated, safe, and complex system at the same time.

The choice of these tools was not just a coincidence, but came after a set of experiments based on the research problem of obtaining a system that has the ability to generate secret, secure, complex, and non-recurring keys and is also characterized by speed while reducing the factors of energy consumption of resources. The following is a review of these tools, which is considered a prelude to understanding the scientific methodology of the current research:

i. Reversible Logic Gates (RLG)

A Boolean function is called "reversible" if and only if every possible combination of inputs has a unique combination of outputs that goes with it. The output state of an RLG digital logic gate is independent of the inputs. Because the injective mapping has the same input and output, RLGs retain their reversible characteristic. The basic RLG set is shown in Fig.1 (a–d), and it consists of a four-input SCL gate, a three-input Fredkin–Toffoli gate, and a two-input Feynman gate. (Table 1) displays the truth tables and functions for all input/output permutations of the RLGs shown in Fig. 1[16].

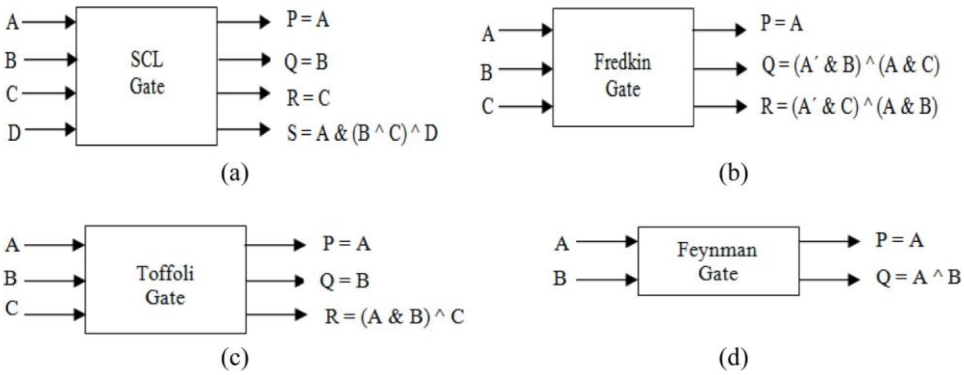


Figure 1. Set of reversible logic gates.
(a) SCL gate with 4 inputs (b) Fredkin gate with three inputs
(c) Toffoli gate with 3 inputs (d) A Feynman gate with 2 inputs.

Table 1. Feynman gate

Feynman gate			
P = AQ = A ^ B			
Input		**Output**	
A	**B**	**P**	**Q**
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Table 2. Toffoli gate

Toffoli gate					
P = *AQ* = *BR* = (A & B) ^ C					
Input			**Output**		
A	**B**	**C**	**P**	**Q**	**R**
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1

Table 3. SCL gate

SCL gate							
P = AQ = BR = CS = A & (B ^ C) ^ D							
Input				**Output**			
A	**B**	**C**	**D**	**P**	**Q**	**R**	**S**
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	0	0	1	0

Table 4. Fredkin gate

Fredkin gate					
P = AQ = (A´ & B) ^ (A & C) ^ (A & B)					
Input			**Output**		
A	**B**	**C**	**P**	**Q**	**R**
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	0	0
0	1	1	0	0	1

ii. XOR Gate

XOR gates are often used in circuits that do math and calculation, especially in half-adders and adders. They are used a lot in computer circuits because they can compare two logic levels and give an output that depends on what the input is. It is not a basic logic gate, but it is used everywhere because it is flexible and useful. Pseudorandom numbers can be generated using a properly configured XOR gate.

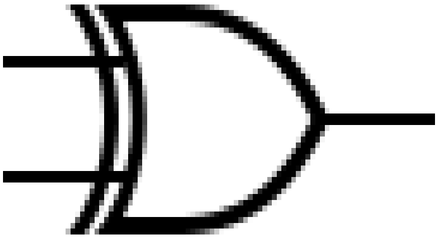


Figure 2. XOR logic gate.

Table 5. XOR truth table

Input		Output
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

iii. Rivest Shamir Adleman (RSA)

The RSA cryptography algorithm is asymmetric. Because it uses two separate keys—the public key and the private key—it is considered asymmetric. The private key is safeguarded from public view, while the public key is made available to everyone who needs it. The difficulty of factoring a large number is the basis of RSA. One of the two numbers making up the public key is the result of multiplying two very large primes. The secret code is also constructed from the same two primes. Therefore, if an adversary factors in the large number, the secret key is compromised. Therefore, the strength of encryption relies solely on the size of the key; tripling or doubling the key size yields an exponential rise in encryption strength. The standard length of an RSA key is 2048 bits; however, experts anticipate that in the near future even this shorter length will be compromised. However, this seems to be an unachievable task at this time [17, 18]. Having large training groups is the key to success for many difficulties in information security, computer vision, and machine learning[19].

iv. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) is a mathematical operation that transforms a signal from its spatial domain to its frequency domain. Since block-based DCT reduces the amount of data needed to reconstruct a digitized image, it is widely used in a variety of digital image and video compression systems. The DCT is a method that JPEG and MPEG use to compress image data by removing extraneous spatial information from two-dimensional images. The conventional JPEG encoding process converts the image's color space from RGB to YCbCr, then divides the image into 8x8 blocks for DCT's spatial-to-frequency transformation; then, using the corresponding constant from the common quantization table, round each DCT coefficient down to the nearest integer. Before moving on to lossless compression, there is a zigzag overview of the DCT's quantized coefficients following this. In each block, the 64 DCT coefficients are laid out from lowest frequency (top left) to highest frequency (bottom right). The higher-frequency details of an image are what really make it pop, while the lower-frequency highlights are where all the action is. The HVS (Human Visual System) is more attuned to low frequencies than high ones.

The Proposed Method

Reversible cryptographic logic is an important field when it comes to optical estimation, discrete-time signal processing, nanotechnology, bio-information, and applications that use little power and don't weigh much. Security is of paramount importance for the aforementioned uses. The parameters of cryptographic protocols in terms of power consumption and physical footprint are also analyzed. Furthermore, the information sent over the connection is vulnerable to being spied on or altered by hackers. In order to avoid this, a reversible logical cipher with the lowest possible cost was constructed, smallest possible footprint, and highest performance power. The symmetric encipher method of RSA makes use of the key generated by the new logic gate system.

The suggested scheme makes use of the same mechanism as[15], but does not make use of LFSR. Additionally, the part of the key generation that is utilized in encryption has been further developed, and the proposed method uses the RSA algorithm to encrypt images. Additionally, it has been using DCT in order to obtain a set of random transactions, particularly from the low-frequency domain. This has been the case throughout.

The proposed method begins with reading the color image and then chopping it up into 8×8 blocks. Next, DCT is applied to those blocks, and finally, a group of coefficients from the low frequency range is selected in order to obtain C_L. C_L represents random coefficients from the low-frequency domain, which will discuss further in this section.

The two procedures of decoding as well as producing the cipher key, which it will benefit from in the encryption stage depending on the RSA technique that will be used later, are the two operations that need to be performed. Our proposed method able to use DCT to select distinct settings for each color image since each color image has its own unique characteristics.

The characteristics of each individual color image are distinct from those of the others. The colored picture could be high- or low-texture, painted, digital, or smoothed. It was take the advantage of this difference in order to obtain new transactions each time, which means that the encryption key will be unique to each image. This, in and of itself, is a source of strength for the proposed method, as it ensures that the key will not be reused. And even though it might be tough to figure out, the proposed procedure is laid out in broad strokes in the figure that will follow:

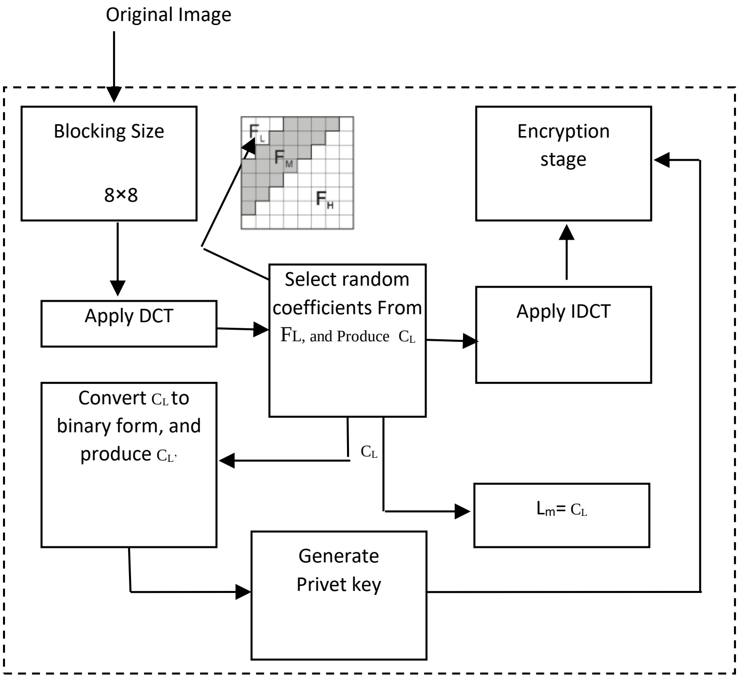


Figure 3. Main diagram of proposed scheme

Where C_L: the selected coefficients (randomly).
F_L: Low frequency domain.
F_M: Middle frequency domain.
F_H: High frequency domain.
L_m: Matrix of the selected coefficients.

Encryption keys are generated using the created logic gate system in Fig.1, and the proposed approach is described below in the form of an algorithm.

Algorithm 1: The proposed Method

```
Input: Original image;
Output: Encrypted Image;
  Begin
    1. Read image as: $O_i$
    2. Split $O_i$ into 8×8 block size, produce $O_{ib}$;
    3. Apply DCT to each block of the whole $O_{ib}$ to produce $O_{ib}'$ ;
    4. From low frequency domain of $O_{ib}'$select random coefficients to produce $C_L$.
    5. $L_m$= $C_L$, where $L_m$ represent the group of selected coefficients.
    6. Generate the privet key after converting $C_L$ to the binary form and produce $C_L'$, then produce $P_k$;
    7. Apply Encryption stage based on $P_k$;
    8. IDCT
    9. By utilizing form $P_k$, Perform encryption stage and produce $O_i'$.
    10. END;: END.
```

Next, generate the encryption key by taking advantage of the developed system, which is dependent on a set of logical gates that increase the complexity of the code generation process.

This process is hard to guess because it uses a complicated method that was developed and used in the proposed method. In the next step, our team will utilize the mechanism that was created in order to determine how to generate the encryption key. The transactions that happen during the DCT phase of the low-frequency domain area, in particular, and the creation of Lm, which has 8 bits, will be split into two equal groups. Each group will have 4 bits and will be spread across two levels of logical gates, starting with the SCL gate and ending with the XOR gate, as shown in the diagram below. This is how Lm will be made. The cipher key that will be used by the RSA method along with the image to finish the encryption phase, as shown in the diagram below:

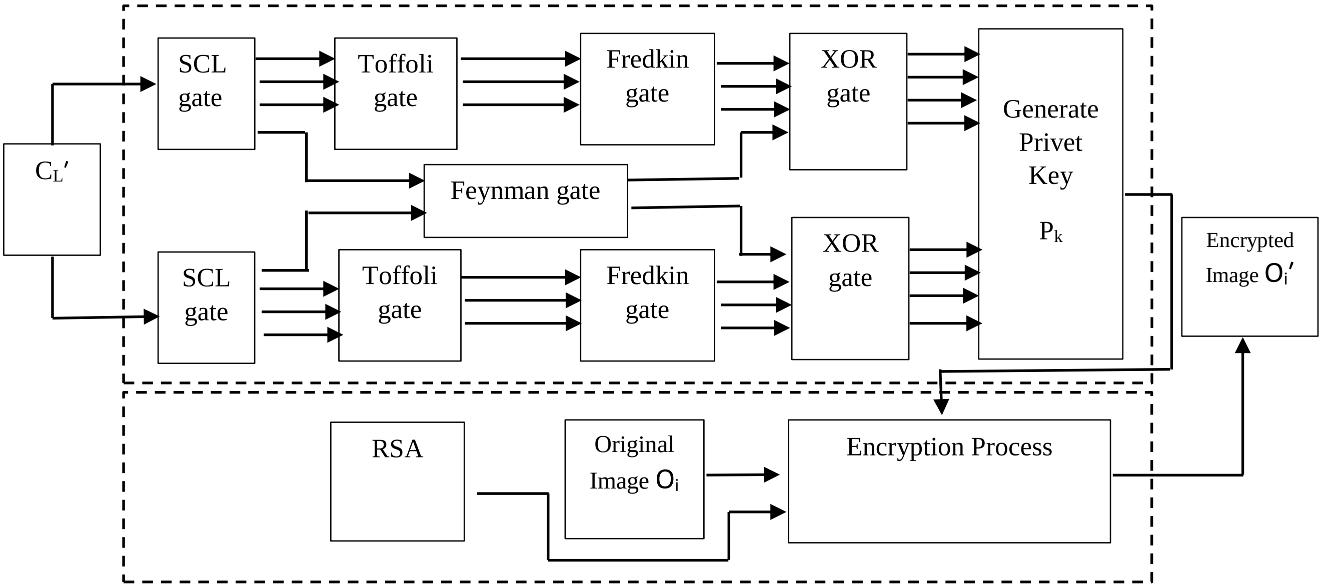


Figure 4. Encryption Stage

The following algorithm shows us the encryption method followed, depending on the methodology that was developed in the process of generating the encryption key, which depends on the type of image used in generating the key used in the encryption process.

Algorithm 2: Encryption Stage

```
Input: Original image, $C_L'$,
Output: Encrypted Image as: $O_i'$.
  Begin
    1. Read image as: $O_i$;
    2. By utilizing $C_L'$, generate the private key as: $P_k$ ;
    3. Apply RSA between $O_i$ and $P_k$ and produce $O_i'$;
    4. END;: END.
```

As shown in Fig. 1 and, Alg 1, the same coefficients will be used to make the decryption key, which is needed to get the original image, as shown in Fig.2.

After getting the encrypted image, you can get the original image by decoding, which depends on Lm, which has the randomly chosen coefficients. Once you have the encrypted image, you can use decoding to get back to the original image.

The process of decoding and getting the image from an encrypted image is described in the following algorithm:

Algorithm 3: Decryption Stage

```
Input: $O_i'$, $L_m$, $P_k'$.
Output: Decrypted Image as: $O_i$.
  Begin
    1. Read image as: $O_i'$;
    2. By utilizing $L_m$, generate the private key as: $P_k'$ ;
    3. Apply RSA between $O_i$ ′ and $P_k'$ and produce $O_i$;
    4. END;: END.
```

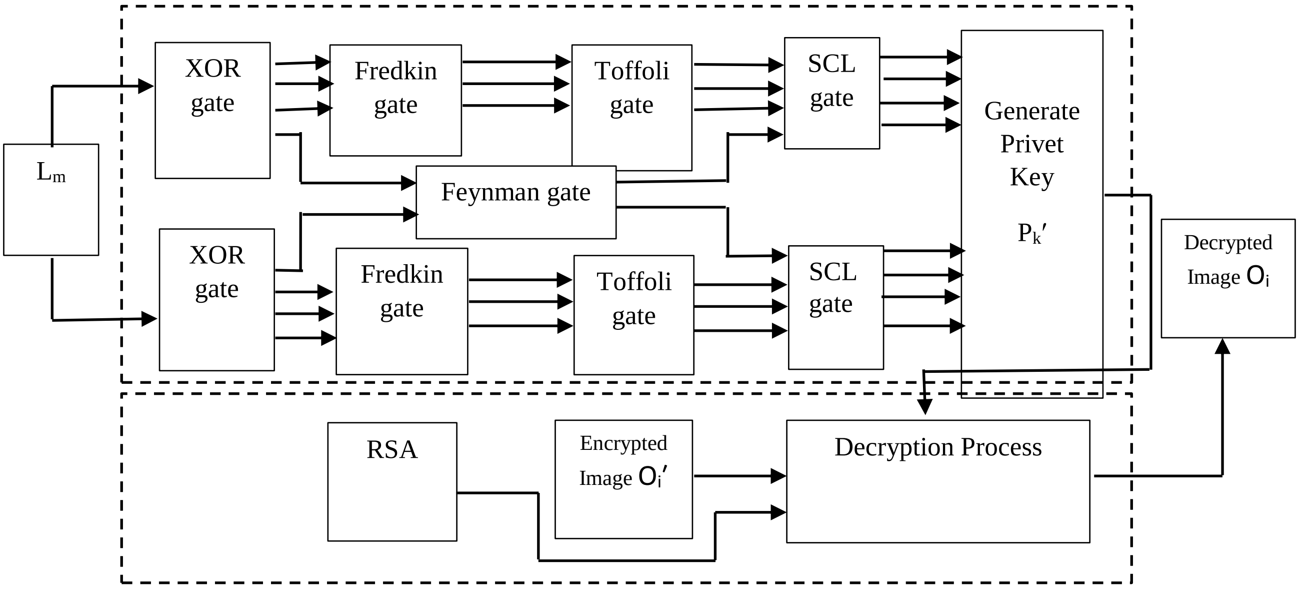
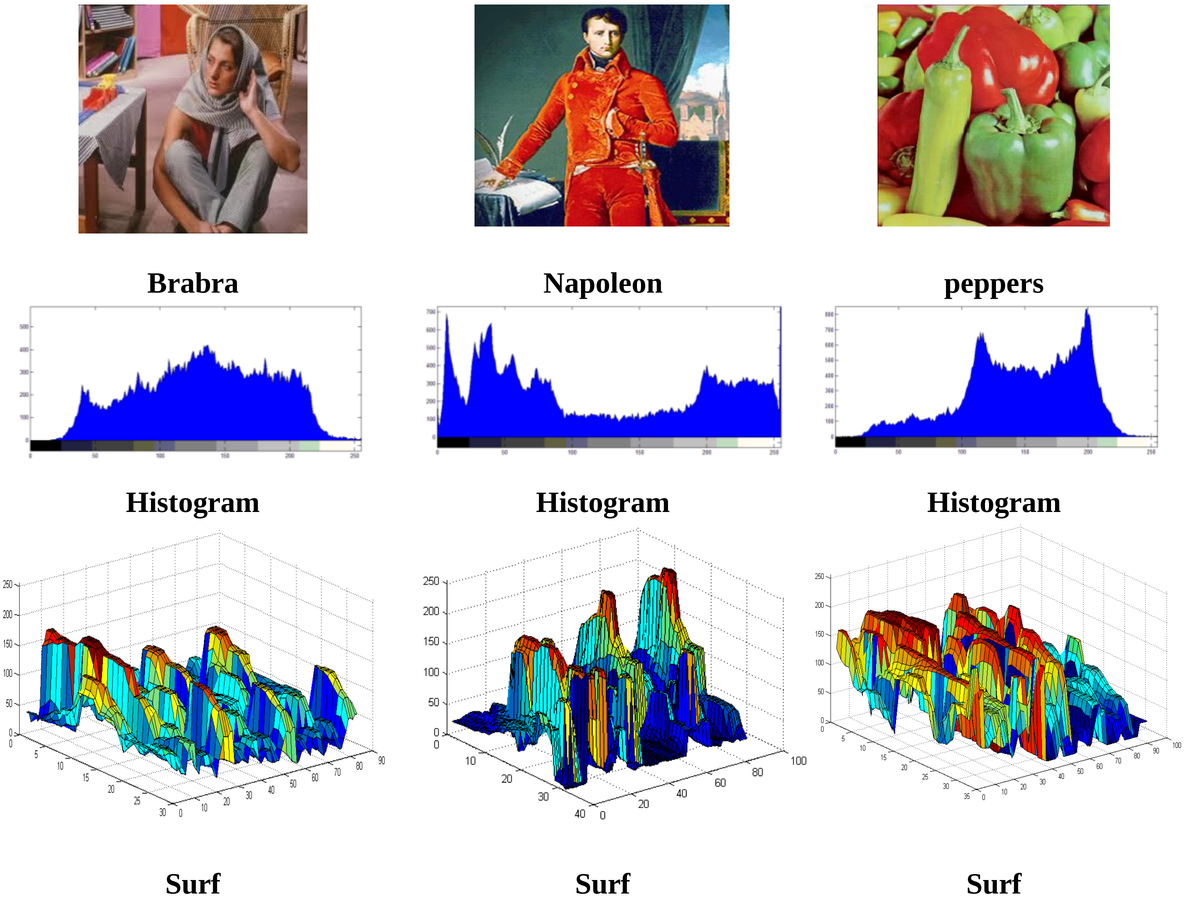


Figure 5. Decryption Stage

Results

In this section, it discusses the proposed scheme's experimental outcomes. Fig. 6 shows the original image with the histogram and the surf. The importance lies in the information presented in (Table 6) in knowing and determining the color nature of image used in the proposed method, although they are all equal in terms of size and type, so that they may later determine the extent to which the contrast between those photographs affected the findings obtained. Which is represented by the different keys that were obtained later in the stage of generating secret keys, on the other hand; (Table 6) shows the image models used in the proposed method along with a summary of the most important features of those models. The evaluation of the proposed method was based on a set of important and common criteria in this field. (Table 7) shows the most important results are got about the size of the image before and after the encoding process and whether or not the encoding process changed the size of the image. (Table 8) shows how long it took to encode and decode the image; on the other hand, Fig. 7 Shows the size variation chart of the encrypted and decrypted images, while Fig. 8 presents the execution time chart. When it looks at Fig. 9, it can see the encrypted image together with its histogram and spectrum. (Table 9) shows the results of an analysis of the image's quality that was done after the decoding process was done.

(Table 10) shows the correlation coefficient, which is used in the statistical analysis. (Table 11) shows the differential attack, which is also used in the statistical analysis. Finally, a comparison between our proposed methods and others is illustrated in (Table 12).



Brabra Napoleon peppers

Histogram Histogram Histogram

Surf Surf Surf

Figure 6. Original image histogram and surf

Table 6. Images properties

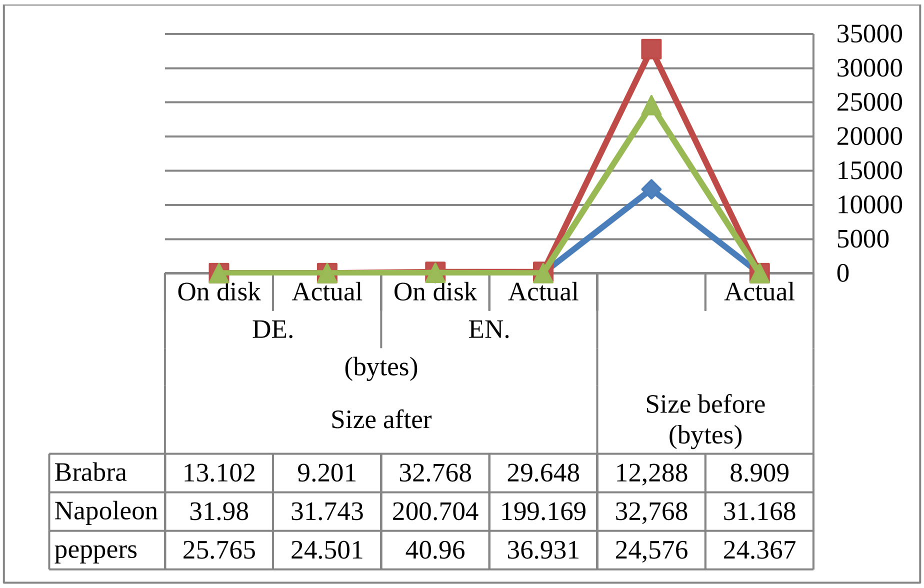
Image	Size	Texture
Brabra	256×256	Smoothed
Napoleon	256×256	Painted
peppers	256×256	High Texture

From the table that presented, were able to see that the images that were used for testing had a wide variety of characteristics. This was done to see how well the proposed method could deal with the differences in how the images seemed to look. The size of the sample does not make a difference in the findings and does not have an impact on the findings in any way.

Table 7. Size variation between encryption and decryption

Image	Size before (bytes)		Size after (bytes)			
			EN.		DE.	
	Actual	On disk	Actual	On disk	Actual	On disk
Brabra	8.909	12,288	29.648	32.768	9.201	13.102
Napoleon	31.168	32,768	199.169	200.704	31.743	31.980
peppers	24.367	24,576	36.931	40.960	24.501	25.765

As for the (Table 7) and Fig. 7, they show the actual and current size of the image before and after the encoding and decoding processes to determine the response of the proposed method to the difference in the size of the image resulting from the different operations and to determine the amount of its effect on the time factor and the degree of complexity.



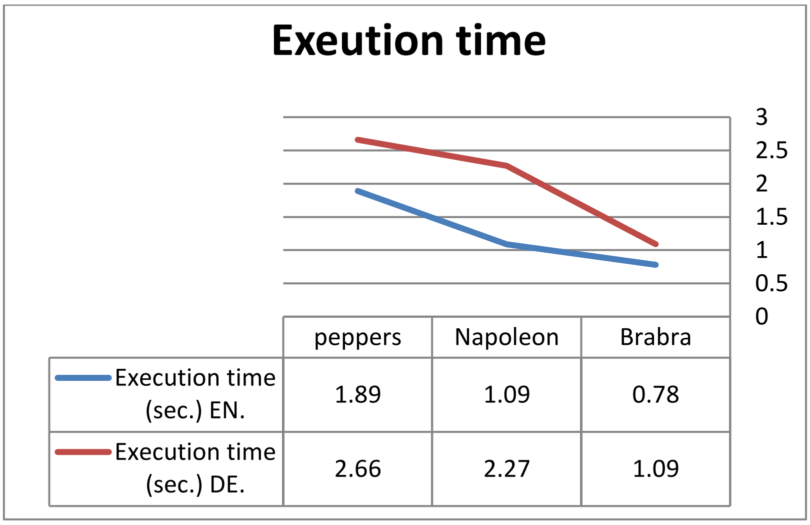
	Size after (bytes)				Size before (bytes)	
	DE.		EN.			
	On disk	Actual	On disk	Actual		Actual
Brabra	13.102	9.201	32.768	29.648	12,288	8.909
Napoleon	31.98	31.743	200.704	199.169	32,768	31.168
peppers	25.765	24.501	40.96	36.931	24,576	24.367

Figure 7. Size variation chart

Table 8. Execution time

Image	Execution time (sec.)	
	EN.	DE.
Brabra	0.78	1.09
Napoleon	1.09	2.27
peppers	1.89	2.66

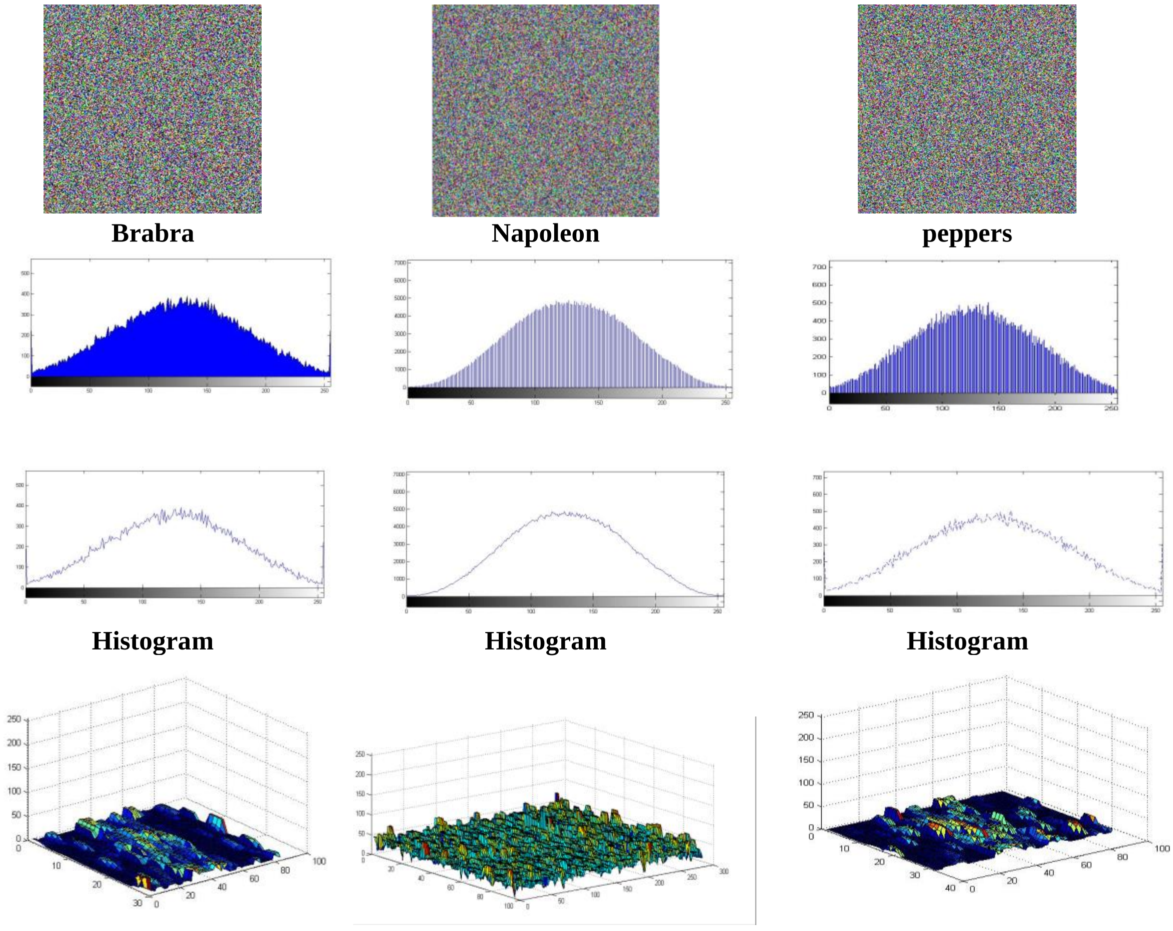
With regard to (Table 8), a high response of the system was observed with the ability to overcome various factors in order to achieve a very good rate of implementation time, which is an important criterion in evaluating the performance level of the proposed system in this field.



	peppers	Napoleon	Brabra
Execution time (sec.) EN.	1.89	1.09	0.78
Execution time (sec.) DE.	2.66	2.27	1.09

Figure 8. Execution time chart

There are many ways of evaluating images after any process is applied to them in order to know the extent of the image's response to that process, including the histogram, which is a well-known and commonly used criterion. Sometimes the response of the image to operations may be very sensitive, and you may need another tool to distinguish it for the reader. This is what happened. With the results that are reviewed, he proposed method used the two types of visible measures to give an integrated idea of the nature of the results that were obtained.



Brabra Napoleon peppers

Histogram Histogram Histogram

Surf Surf Surf

Figure 9. Encrypted image with histograms, and surf.

Apart from image quality analysis based on the visual quality of images encoded by the human eye, there are many comprehensive security analyzes presented in this session that are mainly based on a set of established and well-known criteria such as: List Analysis Mean Square Error (MSE), Peak Signal to Ratio Noise (PSNR), histogram, Curve, and structural similarity index measure (SSIM).

Table 9. Quality analysis (decrypted image)

Image	PSNR	MSR	SSIM	LOSS
Brabra	39.7510	0.9120	0.1134	NO
Napoleon	37.9945	0.3721	0.9812	NO
Peppers	35.2365	1.9923	1.1023	NO

As for the criteria related to the subjective side, the results obtained in this aspect are referred to in Table 9, which contains a set of important, common, and approved standards in this field. It noticed that the quality of the image after the decoding process was not affected and was good, which indicates the success of the proposed method in this test.

In the field of statistical analysis:

A. Correlation Coefficient:

A correlation coefficient of 1 indicates perfect identity between the original and encrypted images. The encrypted image is completely different from the original if the correlation coefficient is 0 (i.e., good encryption). With a correlation coefficient of -1, the encrypted image is the inverse of the original. (Table 10) displays the data gathered from our system.

Table 10. Statistical analysis based on correlation coefficient

Image	Correlation factor
Brabra	0.0073
Napoleon	0.0106
Peppers	0.1449

The results obtained in (Table 10) indicate that the contrast ratio, or difference between the original image and the resulting image after the encoding and decoding processes, is almost nonexistent and does not have any negative effect on the quality of the results.

B. Differential Attack:

Finding out how each algorithm fares under a differential attack is the purpose of this experiment. If a small shift in the plain image can result in a large shift in the cipher image, then a differential attack becomes ineffective, On the other hand; in an attempt to deduce the key, the attacker attempts to discover a relationship between the plain image and the cipher image by examining how variations in an input can affect the subsequent difference at the output. When the attacker attempts to make a minor adjustment, such as changing one pixel of the encrypted image, the plain image changes. Two standards : Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) measurements are used to examine the impact of a single pixel change on the entire encrypted image using the proposed technique, (Table 11) displays the findings of this results.

Table 11. Statistical analysis based on differential attack

Image	NPCR (%)	UACI (%)
Brabra	0.33	0.28
Napoleon	0.77	0.75
Peppers	0.92	0.64

The results collected in (Table 11) show us that the good performance of the proposed system is represented in the high capacity of the proposed system under any differential attack, and the system will not be negatively affected by that, and that differential attack will be ineffective.

Discussion and Analysis

Here, our proposed method introduces a novel encryption method that makes use of DCT, RLG, and XOR. Three different BMP files were used for our tests: Barbra, Napoleon, and Pepper. The experimental results showed that using DCT with RSA achieves comparable key generation with higher PSNR and less MSE than LSFR without RSA and DCT. Simultaneously, it was discovered that LFSR takes a long time for the encryption and decryption processes. On the other hand, attempts in this field are numerous and cannot be compiled into a single study. Based on what is available from sources close to the proposed method and on the principle of modernity in the selection of sources, the proposed method was compared to a group of methods presented in the paragraph of previous studies, and the most significant differences were identified specifically in the field of (image texture and the key encryption domain). Based on the findings of these investigations, the next table summarizes our findings:

Table 12. Comparison with other methods.

Method	Technique (s)	Image texture	Encryption	Key encryption domain
		based	method	
[1]	RLG, LFSR	×	LFSR	Spatial domain
[2]	RLG	×	RC7	Spatial domain
[3]	RLG, LFSR	×	LFSR	Spatial domain
[4]	LFRS	×	LSB	Spatial domain
[5]	RLG,XOR, XTEA	×	DES	Spatial domain
[6]	LFSR	×	X-BOX	Spatial domain
[7]	HIGHT, LED	×	AES	Spatial domain
Our proposed method	RLG, XOR, DCT	Yes	RSA	Frequency/ spatial domain

The using of DCT allows us to generate a very precise and complex key. Moreover, the key length will be indefinite and it attribute the reason for that because the process of generating the secret keys depends heavily in our proposed method on the coefficients that gets from the low frequency region during the DCT phase, which is greatly affected by the chromatic nature of the image (high texture, low texture, painted, digital, and smoothed) and with each type our method will get different parameters. So the feedback to the secret key generator will differ with the difference in the image, and therefore it is possible to obtain a very long key that is difficult to break, which is an important addition and contribution that has not been addressed by much research in this the field.

Conclusion

Our new key generation approach might be used to encrypt and decrypt images by selecting a set of coefficients from a DCT on a color image, notably in the low-frequency domain. High- and medium-frequency domains work well too. It helps us make several keys from a single image or a series of color images based on image texture. Instead, our DCT and RLG phases are key in both the frequency and spatial domains. Our scheme describes an examination of the current condition of modern information security methods like lightweight cryptography. In developing the suggested technique architecture, DCT and RLG were used to convert the image into a frequency domain after randomly selecting it from the mid-frequency domain. A set of random transactions will be passed to a new subsystem consisting of a group of RLG, which is known for its high accuracy and complexity in implementation, its ability to reduce time and resource consumption, and its ability to generate non-static random keys. It is provided to RSA to encrypt once. AES, DES, or other algorithms can be used instead of RSA. Our choice was based on its capacity to shorten implementation time and achieve the desired goals. Since it was changed to another encryption scheme, the results will not be affected. According to the picture texture used for key generation, encryption can take 0.78 to 1.89 seconds and decryption 1.09 to 2.66 seconds. We may generate numerous keys for each image like this.

Acknowledgment

The author(s) would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work, and also the Sfax University, National School of Electronics and Telecommunications of Sfax (ENET'COM), Sfax, Tunisia.

Authors' Declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.

Authors' Contribution Statement

All the research authors worked together to finish this research, and each researcher had an important role that can be summarized briefly: The author **KK** job was to find relevant sources, build the applied side, come to conclusions, make descriptive tables, analyze the results and tables, and compare them to methods that had been used before. On the other hand, researcher **FG** played a major role in writing algorithms and drawing geometric shapes for the research, writing important parts of the research, and taking care of directing and working scenarios. As for the support provided by the researcher **AF**, it was summarized in terms of the linguistic aspect, grammar, and reducing plagiarism and quotation, as well as defining the scientific methodology for the research and drawing the main lines of the research path and providing direct supervision of the article in terms of intellectual and scientific content.

References

1. Ahmed KS, Mohammed HA, Ahmed HM. A New Chaotic Image Cryptosystem Based On Plaintext-Associated Mechanism and Integrated Confusion-Diffusion Operation. Karbala Int J Mod Sci. 2021; 7(3): 176-188. https://doi.org/10.33640/2405-609X.3117
2. Ahmed HM, Ahmed K, Mohammed H. Image Cryptosystem for IOT Devices Using 2-D Zaslavsky Chaotic Map. TEM J. 2022 ; 15(2): 543-553. https://doi.org/10.22266/ijies2022.0430.48.
3. Rawaa MA, Mohammed AH, Amal AK. Detecting Phishing Cyber Attack Based On Fuzzy Rules And Differential Evaluation. J Assoc Inf Sci Technol. 2022; 11(2): 543-551. https://doi.org/10.18421/TEM112-07.
4. Ekhlas Abbas Al-Bahrani, Riyam N.J Kadhum. A New Cipher Based on Feistel Structure and Chaotic Maps. Baghdad Sci J. 2019 ; 16 (1): 270-280. https://dx.doi.org/10.21123/bsj.2019.16.1.
5. Amal AM, Zahraa SD, Raniah AM. Image Confusion and Diffusion Based On Multi-Chaotic System and Mix-Column. Bull Electr Eng Inform. 2021; 10(4): 2100-2109. https://doi.org/10.11591/eei.v10i42924.
6. Abbas EA, Karam TA, Abbas AK. Image Cipher System Based On RSA and Chaotic Maps. Eurasian J Math Comput Appl. 2019; 7(4): 2019 4 – 17. https://doi.org/10.32523/2306-6172-2019-7-4-4-17.
7. Ekhlas A, Riyam NJ. A New Cipher Based on Feistel Structure and Chaotic Maps. Baghdad Sci J. 2019; 16(1): 270-280. https://doi.org/10.21123/bsj.2019.16.1(Suppl.).0270.
8. Jabbar KK, Tuieb MB, Thajeel SA. Digital Watermarking By Utilizing The Properties Of Self-Organization Map Based On Least Significant Bit And Most Significant Bit. Int J Electr Comput Eng. 2021; 12(6): 6545–6558. https://doi.org/10.11591/ijece.v12i6.pp6545-6558.
9. Shailaja A, Krishnamurthy GN. FPGA Implementation and Analysis of RC7 Algorithm Using Reversible Logic Gates. Int J Eng Adv Technol [Internet]. 2019; 8 (6): 769-776. https://doi.org/10.35940/ijeat.F7993.088619.
10. Geethu C, Helen MM, Anjana G. VLSI Implementation of Image Encryption and Decryption Using Reversible Logic Gates. Int Conf Power Electron Renew Energ Appl. 2020; 16 (1): 30-30. https://doi.org/10.1109/PEREA51218.2020.9339781 .
11. Mehran MK, Kaj RA, Siavash BS. Fault Resilient Lightweight Cryptography Block Cipher For Secure Embedded Systems. IEEE Embed Syst Lett. 2014; 6(4): 89–92. https://doi.org/10.1109/LES.2014.2365099.
12. Jabbar, KK, Ghozzi F, Fakhfakh A. Property Comparison of Intellectual Property Rights of Image - Based on Encryption Techniques. TEM J. 2023; 12(1): 529–539. https://doi.org/10.18421/TEM121-63.
13. Z. HA, Guosheng WA, NG. Jain. Security Analysis and Enhanced Design of a Dynamic Block Cipher. China Commun. 2016; 13(1): 150–160. https://doi.org/10.1109/cc.2016.7405712.
14. Srivatsam S, Mehran MK, Reza A, Mehrdad N. Reliable Hardware Architectures For Cryptographic Block Ciphers LED and HIGHT. IEEE Trans Comput-Aided Des. 2017; 36(10): 1750-1758. https://doi.org/10.1109/tcad.2017.2661811.
15. Vinoth R, Siva J, Sundararaman R, Rengarajan A. Security Analysis of Reversible Logic Cryptography Design with LFSR Key on 32-Bit Microcontroller. Microprocess Microsyst. 2021; 84: 1750-1758. https://doi.org/10.1016/j.micpro.2021.104265.
16. Falowo O, Sanjay M, Falayi F, Olusola A, Gokhan S. An Improved Random Bit-Stuffing Technique with a Modified RSA Algorithm for Resisting Attacks in Information Security (RBMRSA). Egypt Inform J. 2022; 23(84): 291–301. https://doi.org/10.1016/j.eij.2022.02.001.
17. Mohammed HA, Ahmed KS, Fadhil HA. An Efficient Confusion-Diffusion Structure For Image Encryption Using Plain Image Related Henon Map. Int J Comput. 2020; 19(2): 1-3. https://doi.org/10.47839/ijc.19.3.1895.
18. Enas FK, Eklilas FN, Alaa NM. Comparison between RSA and CAST-128 with Adaptive Key for Video Frames Encryption with Highest Average Entropy. Baghdad Sci J. 2022; 19 (6): 1378-1386. https://doi.org/10.21123/bsj.2022.6398
19. Mukesh S, Marwan AS, Yoshua B.Scalable Neural Network Algorithms for High Dimensional Data. J Big Data . 2023: 1–12. https://doi.org/10.58496/MJBD/2023/001.

2023, 20(6 Suppl.): 2593-2607
https://dx.doi.org/10.21123/bsj.2023.8715
P-ISSN: 2078-8665 - E-ISSN: 2411-7986

Baghdad Science Journal

نظام قوي لتشفير الصورة الملونة بالاعتماد على RSA من خلال DCT بأستخدام نهج تصميم منطقي متقدم

خالد كاظم جبار [1]، فهمي كوزي[2,3] ، أحمد الفخفاخ[2,3]

[1]قسم علوم الحاسوب، كلية التربية، الجامعة المستنصرية، بغداد، العراق.
[2]قسم الإلكترونيات ، المدرسة الوطنية للإلكترونيات والاتصالات بصفاقس ،جامعة صفاقس, صفاقس, تونس.
[3]مختبر الإشارات والأنظمة والذكاء الاصطناعي والشبكات (SM @ RTS) ، مركز البحوث الرقمية بصفاقس (CRNS) ، صفاقس ، تونس.

الخلاصة

تتزايد أهمية أمن المعلومات في تخزين البيانات ونقلها. من جانب اخر يتم استخدام الصور في العديد من الإجراءات. لذلك ، يعد منع الوصول غير المصرح به إلى بيانات الصورة أمرًا بالغ الأهمية من خلال تشفير الصور لاجل حماية البيانات الحساسة او الخصوصية. تتنوع طرق وخوارزميات إخفاء الصور أو تشفيرها من طرق المجال المكاني البسيطة إلى طرق مجال التردد والذي يعتبر الأكثر تعقيدًا وموثوقية. في هذا البحث ، نقترح نظام تشفير جديد يعتمد على منهجية تهجين مولد المفتاح العشوائي من خلال الاستفادة من خصائص DCT لتوليد مجموعة غير محددة من المفاتيح العشوائية والاستفادة من معاملات المنطقة منخفضة التردد بعد مرحلة DCT لتمريرها إلى نظام فرعي يتكون من مجموعة RLG للحصول على المفاتيح السرية التي يتم تمريرها إلى RSA لتنتهي بتشفير الصورة.
تشير النتائج إلى أن الطريقة المقترحة لها القدرة على تولد مجموعة كبيرة جدًا من المفاتيح السرية شديدة التعقيد والآمنة التي يمكن استخدامها لاحقًا في مرحلة التشفير. علاوة على ذلك ، سيتغير عدد وتعقيد تلك المفاتيح في كل مرة يتم فيها تغيير الصورة، وهذا يمثل مساهمة الطريقة المقترحة. ولم نلاحظ اي ضياع للوقت أثناء عمليات التشفير وفك التشفير لاستخدامنا RLG ، مما يدل على أن النظام المقترح قام بعمل جيد في صنع مفاتيح مختلفة من نفس الصورة. ويختلف في قوة المفتاح من صورة إلى أخرى حسب طبيعة الصورة الملونة.

الكلمات المفتاحية: نظام التشفير, فك التشفير ,تحويل الجيب تمام , التشفير, البوابات المنطقية العكسية, ريفست شامير أدلمان.