Mustansiriyah Journal of Pure and Applied Sciences

www.MJPAS.com

Image Encryption Performance Analysis Using Reversible Logic Gates

K. K. Jabbar[*1] F.Ghozzi[2,3] A .F. akhfakh[2,3]

[1]Computer Science Department, Collage of Education, Mustansiriyah University, Baghdad, Iraq.(khalidk.jabbar@uomustansiriyah.edu.iq)
[2]Departement of Electronic, National School of Electronics and Telecommunications of Sfax, University of Sfax,Tunisia(fahmi.ghozzi@gmail.com)
[3]Laboratory of signals, Systems, Artificial intelligence and Networks (SM@RTS), Digital Research Center of Sfax (CRNS), Sfax, Tunisia. (ahmed.fakhfakh@enetcom.usf.tn)

A B S T R A C T

Information security is one of the important sciences that needs great attention from professionals in this field because of the growing need to use the WWW (World Wide Web) and the growing human connection with it. It is urgent to take advantage of the services that are provided through the network. With this in mind, we set out to review and compare several new papers examining the use of RLG (Reversible Logic Gates) to encode images. Due to the fact, that attempts in this field are few compared to multiple attempts in other fields, we highlighted eight studies published between 2013 and 2022, we compared this studies and our analysis consider a wide range of factors, including but not limited to the encryption technology, logic gates used, image size, key length, portable data volume and security analysis.

The results, that mentioned in the tables, show that most businesses use common encryption algorithms with some traditional additions that make the systems more efficient and innovative. This is especially true for systems that use reversible logic gates to encrypt data based on chaotic permutations, difference equations, and other methods. The comparison also shows the downsides and trade-offs of each method, such as how increasing the size of an image affects the time it takes to encrypt it and how important it is to find a balance between security and performance. Overall, the study provides useful information in the field of image coding via using inverse logic gates and suggests possible directions for future work.

Keywords: *Information security, WWW, Logic gate, RLG and Encryption.Article history*

Received: Received in revised format: Accepted Available online.

1. Introduction

Encryption is one of the most important data privacy, security, and protection against unwanted access technologies. A reversible logic gate is one of the main security-enhancing innovations [1].

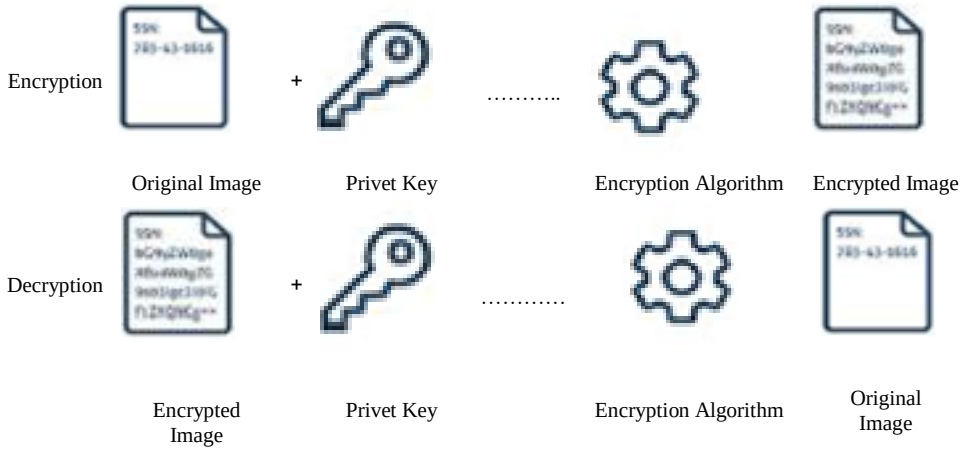

Figure 1. Simple encryption and decryption process [13]

The encryption process focuses on one concept, which is the process of converting sensitive data or information into an incomprehensible format, with attention to many factors that will increase the quality of the proposed system, such as attention to the security aspect, increased complexity, time factor, resource consumption, and adaptation to the ever-changing data type. Hence, many various proposals and contributions are emerged, and each of them had advantages that solved many problems related to the security aspect and prevented intruders from controlling important systems in order to preserve the important data stored in them. On the other hand, intruders and information thieves will not hesitate to develop methods of acquiring secure systems by penetrating them and bypassing all the security and confidentiality walls of those systems. This is another challenge for developers or those interested in this field that represents the need to develop effective systems that have the ability to maintain sensitive information in a secure manner that cannot be hacked by hackers. The reversible logic operation creates zero power loss and supplies information without any loss. In order to prevent data loss, the output of each reversible logic gate is drawn from its input. Image encryption is the process of changing an image into a format that can't be read [2]. Using cryptography and encryption methods, It is possible to use cryptography.

The information is decrypted using the same method and key. Images can be encrypted to prevent tampering with or viewing of private information. The importance of digital photographs has grown as they have become more widely available. However, encryption has been employed with many different types of software that deal with images on a regular basis (such as military and government software, financial organizations, healthcare providers, and others) to ensure that the data they contain remains private [3].

Encrypting photos is a simple yet effective way for businesses to safeguard their data from prying eyes. Plain text mechanisms, random substitution boxes, chaotic systems, Feistel structures, Henon maps, two-dimensional chaotic Zaslavsky maps, and Playfair codes are just some of the methods and techniques that have been tried in the field of image coding [4-11]. There are many advantages that must be available in the RLG, including:

- Reversible Function: When the number of outputs matches the number of inputs, the Boolean function $F(x_1; x_2,..., x_n)$ is said to be reversible. There is a unique pre-image

for each possible output pattern. Reversible functions specifically execute permutations of the input vector set.

- Reversible logic: In a reversible logic circuit, the same number of outputs matches each input. As a result, for any given set of input vectors, a unique set of output vectors is produced.
- Garbage outputs: The number of inputs and outputs can be equalized by adding more of any type of input or output as needed. Garbage is the additional number of outputs required to make a function with m inputs and k outputs ((m; k) function) reversible. Below is the formula relating the total number of trash outputs to the total number of constant inputs:

  Input + constant input = output + garbage

  The term "garbage line" is used to describe an output line that must be present in order for reversibility to be maintained [12-15].
- Quantum Cost: The quantum cost of converting a classical circuit into a quantum circuit is the amount of work required to make that transition. The number of primitive reversible logic gates required to deduce the circuit's identity is used in the calculation.
- Constant inputs: also known as ancillary inputs are those that are always held at either 0 or 1 in order to implement the specified logical function.
- Flexibility: A reversible logic gate's universality allows it to realize a wider variety of purposes, which we call flexibility.
- To recognize the specified logic operations, a particular circuit must have a certain "gate level."
- Complications in the Hardwareof a circuit is defined as the sum of all its logical opera tions.That is, the sum of all AND, OR, and EXOR gates in a circuit [16].

2. The reversible logic gates

Many fields, including cryptography, can benefit from the use of a reversible logic gate. These gates are essentially a collection of logical circuits that may be used to process data and then reverse that processing. Using this technique, we are able to encrypt the data while preserving its original form. The topic of image encryption makes extensive use of reversible logic gates since they allow us to encrypt more securely than conventional methods. The most common reversible logic gates are the SCL gate, Friedkin gates, and Feynman gates. One of the most fundamental reversible logic gates, Toffolie gates, is employed in the encoding and decoding processes. The random numbers produced by the more sophisticated Friedkin gates can be utilized as encryption keys. When it comes to encrypting sensitive information, the most complicated inverse logic gate type is the Feynman gate.

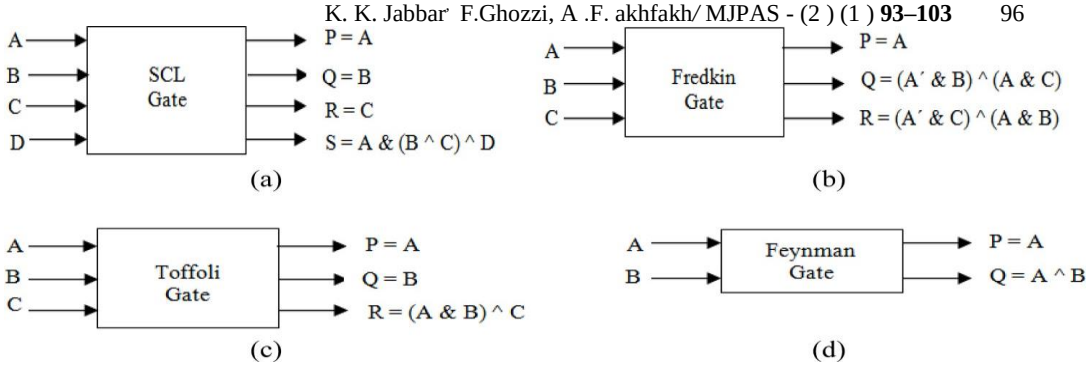

Figure 2. The reversible logic gates. (a) SCL gate with 4 inputs (b) Fredkin gate with three inputs (c) Toffoli gate with 3 inputs (d) A Feynman gate with 2 inputs.

In order to achieve more nuanced outcomes from data processing, "reverse logic gates" are employed. However, using this technology, they can encrypt data without altering it in any way.

The first step in the encryption process is for the reversible logic gate to read the information. A collection of logic circuits including AND, OR, NOT, and XOR gates then processes this information.

The data is encrypted when its outputs are fed into a logic circuit that generates the encryption key. The data can then be decrypted back to its original form with no information being lost due to the reversal of the encryption process [17].

3. How RLG Improve Image Encryption Security

Generally speaking, image encryption is the process of converting an image into an unreadable format for hackers. This technique is employed to safeguard sensitive data from intrusion. Data encryption and decryption rely on cryptographic algorithms and cryptographic keys. Engineers utilize reverse logic gates to increase the complexity of key generation and strengthen cryptographic processes. One of the most important criteria required for the success of any image encryption algorithm depends on the principle of permeation. By increasing randomness, preventing repetition, and consuming the least possible resources and energy while preserving the image quality after the encryption process, in addition to increasing the complexity as much as possible, we can meet all of these criteria.

It is done by using RLG when building image encryption systems or encryption systems in general, especially for images. Using logical gates when building systems that encrypt images makes those systems more efficient, keeps their structure strong against attacks, and makes the proposed method or system more integrated. Therefore, we will obtain a system that has the ability to protect itself and perform the tasks assigned to it [18].

There are several positive aspects to this. Most importantly, using reverse logic gates in image encryption greatly improves security while reducing the risk of data loss. This is because the original data can be recovered when encryption is complete, as the encryption process is reversible. In addition to being more effective than conventional cipher methods, reversible logic gates also require fewer resources than the processing capability of a computer. This makes them appropriate for uses where haste and effectiveness are

paramount. Reversible logic gates also allow for more secure encryption, which is a nice perk. Reversible gates allow for more secure encryption, because they use more gates. This strengthens the encryption, because it makes decryption more complex. Random numbers generated with reversible logic gates can be utilized as cryptographic keys for picture encryption.

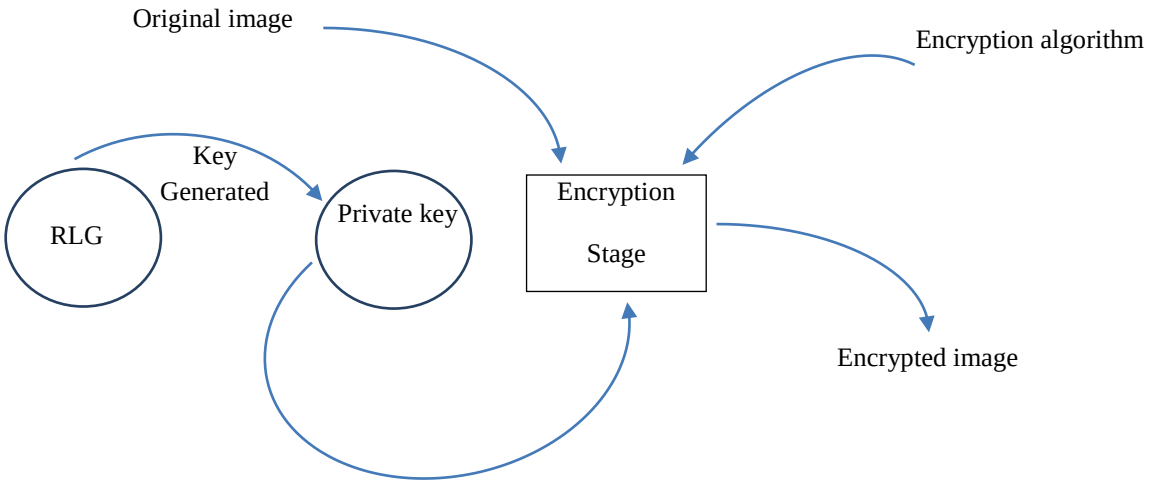

Figure 3. General diagram of image encryption using RLG

4. Applications of RLG in Image Encryption

The most prevalent application of reversible logic gates is picture encryption. Using reversible logic gates, it is possible to encrypt and decrypt images consistently. They can also be used to produce random numbers for use as cryptographic keys in picture encoding. Images can be compressed and altered with the help of reversible logic gates. This can be helpful for apps that need a small, safe way to store and send images.

Image encryption makes extensive use of reversible logic gates. For instance, the AES-256 method employs both Toffoli and Fredkin gates in its encryption and decryption processes. The ECC-256 encryption technique is another such; it uses Feynman gates to produce random numbers for use as cryptographic keys. Finally, there are a number of open-source tools and packages available for developers who are interested in employing reversible logic gates for picture encryption. For instance, the OpenCL package provides a set of application programming interfaces that can be used to implement one's own reversible logic gates. Many research articles and tutorials are also available online to assist programmers in learning how to use reversible logic gates.

5. Points of strength and weakness of RLG

There are various benefits to reversible logic gates over traditional encryption methods. To begin, they make better use of time and energy because they demand less hardware and software. This makes them appropriate for uses where haste and effectiveness are paramount.

Second, they provide more secure encryption. Reversible gates allow for more secure encryption because they use more gates. This strengthens the encryption because it makes decryption more complex. Random numbers generated with reversible logic gates can be utilized as cryptographic keys for picture encryption. They are also more malleable than most.

Data encryption and decryption are just two of the many possible uses for reversible logic circuits. This affords programmers greater flexibility when designing cryptographic protocols. Although reversible logic gates have many advantages, they also have certain disadvantages. For starters, they are more sophisticated than typical encryption methods, making them harder to utilize for unskilled developers. Furthermore, the intricacy of the logic gates can make debugging more challenging. Second, reversible logic gates need extra resources to function. This can be a problem for apps with restricted resources.

Finally, because they require specific hardware and software to function, reversible logic gates can be costly [19].

6. Related work

A.C. Nuthan et al. (2013) provide a practical method for the design of DES with reversible gates. A Feynman gate can be utilized to create the proposed design.

This suggested data encryption standard with reversible logic gates eliminates bit information loss and reduces power consumption in comparison to the present data encryption standard with conventional logic gates. The suggested architecture offers less hardware complexity, a lower gate count, fewer garbage bits, and consistent inputs.

By fault-proofing each submodule, it may be possible to make the same design fault-tolerant in the future. As this is developed on an FPGA, it can be deployed on an ASIC effectively in the future [12]. Whereas R. Bapannadora et al. (2017) present a method for the creation of encryption algorithms based on reversible logic. An encryption strategy is a component of the 4-input cascade of reversible gates in the proposed solution. In this manner, the fourth building component, variable function, is reversible. Proposed for this purpose is a changeable gate. The design by CNOT, Toffoli, and Friedkin [13], has been presented since this type of reconfigurable gate is constructed using ordinary reversible materials.

Saranya et al. [14] the architecture for reversible logic cryptography design (RLCD) is introduced in this work. Encryption and decryption architectures are created with the aid of RLCD. The encryption and decryption blocks require a key that is generated via a linear feedback shift register (LFSR). Existing and proposed application-specific integrated circuit (ASIC) and field-programmable gate array (FPGA) performance evaluations are conducted. The RLCD-LFSR approach enhanced the performance of ASICs by more than 7 percent compared to conventional methods. Abdulmajeed A.Y. et al. [15] present a comprehensive analysis of the implementation of field-programmable gate arrays (FPGAs) using DES and AES; moreover, Geethu Chandran et al. [16] RLGCD is utilized in both the encryption and decryption architecture design processes. A shift register with linear feedback are used to create the key for encryption and decryption procedures. The Least Significant Bit (LSB) approach is utilized for watermarking to further enhance the security of data. The RLGCD

architecture's FPGA performance is assessed. The performance of the RLGCD design is much superior to that of other traditional systems.

B. Murali Krishna et al. [17] show an image cryptology (IC) with a secret key built with runtime linear feedback shift register logic (RLFSRL) for encrypting and decrypting data with reversible logic gates (RLG) on a field-programmable gate array (FPGA).

Edge detection-based cryptanalysis proposed in [18] is enough to crack the Reversible Logic Cryptography Design (RLCD)-Linear Feedback Shift Register (LFSR) scheme. Adding a confusion module to the Reversible Logic Cryptography Design (RLCD)-LFSR scheme removes patterns and edges from encrypted images to stop attacks.

The fact that expanded RLCD-LFSR failed NIST tests shows that the Reversible Logic Gate (RLG)-based diffusion mechanism for picture encryption has problems with its design and doesn't work well. In addition to the security analysis, the RLCD-LFSR scheme and its proposed improvement are tested on a 32-bit microcontroller to see if they are good for real-time embedded applications.

Based on the random difference equations, random permutations, and randomized logic circuits in [19], a method for encrypting pictures that works well and won't break easily is created. To produce pseudo-random sequences, hyper-chaotic and chaotic systems are utilized.

These sequences are used to create random first-order difference equations, chaotic permutations, and logic circuits. Image encryption based on these three random modules is simple to decipher and secure against statistical, differential, and chosen-plaintext attacks.

7. Discussion and analysis

Our study looks at how eight research papers on image encryption using reversible logic gates compare to each other. The works that were looked at cover different parts of the topic, such as how encryption algorithms are used, how field-programmable gate arrays (FPGAs) are used, and how encryption schemes' security is analyzed. The comparison is based on a number of things, such as the encryption algorithm, the logic gates used, and the size of the image, the length of the key, the throughput, and the security analysis. The results show that most of the works looked at use the Advanced Encryption Standard (AES) algorithm with different kinds of reversible logic gates to encrypt images in a way that is fast and safe. But some studies also suggest new encryption methods based on chaos and difference equations. The comparison shows how important it is to think about both security and performance when making reversible logic gate-based image encryption systems.

Attempts in this field are many and varied and cannot be collected in one study. Also, having the same information in more than one place makes the research less scientific.

So, we tried to find a mix of modern and older sources so that we could learn more about them and make a simple, scientific analysis by comparing them. These methods interact with each other, as shown in the following two tables:

Table 1. Comparison according to the several aspects

Method	Encryption Algorithm(s)	Reversible Gates	Key Length(s)\ Bits	Input Size	Output Size	Performance (Speed)\ Gbps
[12]	DES	Fredkin and Toffoli gates	56	64 bits	64 bits	3.67
[13]	AES	Reconfigurable TSG and Toffoli gates	128/192/256	128 bits	128 bits	17.89
[14]	Reversible Crypto Gates	Reversible Full Adder and Fredkin gates	128	8×8 pixels	8x8 pixels	Not specified
[15]	DES	Fredkin and Toffoli gates	56	Not specified	Not specified	Not specified
[16]	Image encryption	Fredkin and Feynman gates	256	256×256	256x256	Not specified
[17]	Image encryption	Reversible Full Adder, Reversible Half Subtractor gates	128	512×512	512x512	Not specified
[18]	Reversible Crypto Gates	Fredkin and Toffoli gates	128	Not specified	Not specified	Not specified
[19]	Image encryption	Reversible Full Adder and Fredkin gates	128	256×256	256x256	Not specified

While the table below shows a more detailed comparison of how each study was done and what techniques were used for reversible logic gates, such as approach, key generation, data block cipher, input/output, image encryption, key features, and limitations:

Table 2. Comparison according to specific techniques

Method	Approach	Key Generator	Block Cipher	Input Data	Output Data	Image Encryption	Key Features	Limitations
[12]	DES	LFSR	ECB	Binary	Binary	No	Focus on minimizing the number of gates with limited evaluation and comparison.	Limited analysis of security and efficiency
[13]	AES	LFSR	ECB	Binary	Binary	No	Focus on minimizing the number of gates and increasing throughput, but limited evaluation and comparison	No analysis of security
[14]	Custom	LFSR	CBC, OFB, CFB	Binary	Binary	No	Focus on designing a new reversible logic gate and evaluating its security and performance.	Limited experimental evaluation
[15]	DES	Custom	CBC, CTR	Binary	Binary	No	Survey of existing FPGA implementations and evaluation of their performance and throughput	No analysis of security
[16]	Custom	Custom	CBC, CTR	Image	Image	YES	Focus on designing a new reversible logic gate and applying it to image encryption.	Limited analysis of robustness
[17]	Custom	Custom	ECB, CBC	Image	Image	YES	Focus on applying reversible logic gates to image encryption and evaluating the security and performance.	Limited analysis of security and efficiency
[18]	Custom	Custom	-	Image	Image	YES	Focus on designing a new	Limited

							image encryption scheme using chaotic permutations and reversible logic gates.	experimental evaluation
[19]	Custom	Custom	-	Image	Image	YES	Focus on evaluating the security of reversible logic gates and LFSR key generation.	Limited experimental evaluation

Notes:

- Approach: the type of encryption algorithm used (e.g., DES, AES, custom).
- Reversible Gates: the type of reversible logic gates used (e.g., Toffoli, Fredkin, Peres)
- Key Generator: the type of key generator used (e.g., LFSR, custom).
- Block Cipher: the mode of operation used for block ciphers (e.g., ECB, CBC, and CTR).
- Image Encryption: whether or not the encryption algorithm is designed specifically for image encryption

Using this methods, images are encrypted using differential equations, chaotic permutations, and logic gates. It has been demonstrated to be an effective and trustworthy encryption technique. The results of the study demonstrate that images could be encrypted in a secure and energy-efficient manner by employing reversible logic gates. The use of reversible gates allows for the creation of numerous encryption schemes. Encryption systems are based on reversible logic gates are strengthened by LFSRs and chaotic permutations. Security and efficiency improvements have been demonstrated in FPGA and VLSI implementations of reversible logic gates for image encryption.

8. Conclusion

The introduction of reversible logic gates has led to a rise in the popularity of image encryption. They provide for more flexibility in the creation of encryption algorithms, faster processing, and more secure encryption, among other benefits.

Tools and resources abound to aid developers in their use of reversible logic gates. Businesses can ensure the security of sensitive data by encrypting photos with reversible logic gates. Consider employing reversible logic gates to encrypt your photographs for a more secure and time-saving solution.

- Because they can switch the order of their inputs and outputs, reversible logic gates are becoming more popular in the field of picture encryption. This allows you to decrypt an encrypted image without losing any data.
- The security of systems that use reversible logic for encryption depends on the logic gates used and how they are set up, as well as the size and randomness of the encryption key. Many researchers think that the encryption method could be implemented in hardware using field-programmable gate arrays (FPGAs), which would allow for high throughput while using little power.

Even though AES is a popular encryption standard for reversible logic-based image encryption, work is still being done to create more secure and efficient encryption algorithms for reversible logic gates.

• The analysis indicates that more research is needed on the trade-offs between security and performance in reversible logic-based image encryption, as well as how different image sizes and kinds affect the time it takes to encrypt and decrypt images.

Different studies use reversible logic gates to encrypt images in different ways, and there is no clear agreement on the optimal technique to do so. The application and its needs will tell you which encryption algorithm, logic gates, key size, and performance metrics to use. An analysis of security is an important part of any encryption method, and more research is needed to find out how strong the encryption algorithms described in these papers are.

It is possible to present a set of proposals for future work in this field that may contribute to the development of the proposed encryption systems and enhance the security aspect of those systems. From this point of view, we suggest that the system be built in the transform domain, and here we show the possibility of using DCT or DWT, DFT, FFT, and others, which can improve the performance of the proposed system and is considered a scientific addition in this field. Moreover, we can use the chaotic system in the key generation process in addition to the reversible logic gates, and we should not forget the comparison after a deep analysis of the results, which may constitute an important turning point in building such types of effective encryption systems.

Acknowledgement

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.

9.Reference

[1] Shakir, H. R., Mehdi, S. A., & Hattab, A. A. (2023). A New Method for Color Image Encryption Using Chaotic System and DNA Encoding. Mustansiriyah journal of pure and Applied Sciences, 1(1), 68-79.

[2] Jabbar, K. K., Munthir, B. T., & Thajeel, S. A. (2022). Digital watermarking by utilizing the properties of self-organization map based on least significant bit and most significant bit. International Journal of Electrical and Computer Engineering, 12(6), 6545.

[3] Jabbar, K. K., Ghozzi, F., & Fakhfakh, A. (2023). Property Comparison of Intellectual Property Rights of Image-Based on Encryption Techniques. TEM Journal, 12(1).

[4] Jabbar, K. K., Munthir, B. T., & Thajeel, S. A. (2022). Digital watermarking by utilizing the properties of self-organization map based on least significant bit and most significant bit. International Journal of Electrical and Computer Engineering, 12(6), 6545.

[5] Alshekly, T. K., Albahrani, E. A., & Lafta, S. H. (2022). 4d chaotic system as random substitution-box. Multimedia Tools and Applications, 81(11), 15793-15814.

[6] Chalob, D. F., Maryoosh, A. A., Esa, Z. M., & Abbud, E. N. (2020). A new block cipher for image encryption based on multi chaotic systems. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(6), 2983-2991.

[7]. Al-Bahrani, E. A., & Kadhum, R. N. (2019). A new cipher based on Feistel structure and chaotic maps. Baghdad Science Journal, 16(1), 270-280.

[8]. Al-Bahrani, E. A., & Kadhum, R. N. (2019). A new cipher based on Feistel structure and chaotic maps. Baghdad Science Journal, 16(1), 270-280.

[9] Albahrani, E. A., Maryoosh, A. A., & Lafta, S. H. (2020). Block image encryption based on modified playfair and chaotic system. Journal of Information Security and Applications, 51, 102445.
[10] Maryoosh, A. A., Dhaif, Z. S., & Mustafa, R. A. (2021). Image confusion and diffusion based on multi-chaotic system and mix-column. Bulletin of Electrical Engineering and Informatics, 10(4), 2100-2109.
[11] Mohammed, A. H., Shibeeb, A. K., & Ahmed, M. H. (2022). Image Cryptosystem for IoT Devices Using 2-D Zaslavsky Chaotic Map. International Journal of Intelligent Engineering & Systems, 15(2).
[12] Nuthan, A. C., Nagaraj, C., & Havyas, V. B. (2013). Implementation of data encryption standard using reversible gate logic. International Journal of Soft Computing and Engineering, 3(3), 270-272.
[13]. Dey, J. (2022). COVID-19 paediatric cavity telecare system: a novel chain key generation and encryption scheme. International Journal of Reconfigurable and Embedded Systems, 11(1), 13.
[14] Karunamurthi, S., & Natarajan, V. K. (2019). VLSI implementation of reversible logic gates cryptography with LFSR key. Microprocessors and microsystems, 69, 68-78.
[15] Karunamurthi, S., & Natarajan, V. K. (2019). VLSI implementation of reversible logic gates cryptography with LFSR key. Microprocessors and microsystems, 69, 68-78.
[16] Chandran, G., Mary, H., & Anjana, G. (2020, November). VLSI Implementaion of Image Encryption and Decryption Using Reversible Logic Gates. In 2020 International Conference on Power Electronics and Renewable Energy Applications (PEREA) (pp. 1-6). IEEE.
[17] Krishna, B. M., Kavya, K. C. S., Kumar, P. S., Karthik, K., & Nagababu, Y. S. (2020). FPGA implementation of image cryptology using reversible logic gates. Int. J. of Advanced Trendsin Computer Science and Engineering, 9(3).
[18] Raj, V., Janakiraman, S., Rajagopalan, S., & Amirtharajan, R. (2021). Security analysis of reversible logic cryptography design with LFSR key on 32-bit microcontroller. Microprocessors and Microsystems, 84, 104265.
[19] Annaby, M. H., Ayad, H. A., & Rushdi, M. A. (2022). A Difference-Equation-Based Robust Image Encryption Scheme with Chaotic Permutations and Logic Gates. Journal of Mathematical Imaging and Vision, 64(8), 855-868.