Property Comparison of Intellectual Property Rights of Image - Based on Encryption Techniques

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

[1] *Mustansiriyah University, Collage of Education, Computer Science Department, Baghdad-Iraq*
[2] *Département Électronique École Nationale d'Electronique et des Télécommunications de Sfax, Tunisia*
[3] *Digital Research Center of Sfax (CRNS), Laboratory of signals, systems, artificial intelligence and networks, (SM@RTS), Sfax, Tunisia*

Abstract **– The term of Intellectual Property Rights (IPR) refers to the legal protections attached to works of creativity, such as image, books, movies, and music. The purpose of IPR is to ensure that the people responsible for creating anything new have the opportunity to profit from their labor. Different forms of IPR protection exist, such as: patents, copyrights, trademarks, etc. Our comparison presents some solutions for IPR based on image encryption that might improve the security of online communities with regards to intellectual property of images. It can be used to help ensure and that multimedia content is used legally under the terms of the copyright license selected by the content creators. Copyright issues can be found and reported more quickly with its help. In any case, multimedia files are crucial to the functioning of the modern internet. Encrypting this information is a great way to keep it safe. It will soon be an integral part of the safeguards protecting the integrity of the internet.**

Keywords **– Intellectual Property Rights, image encryption, patents, copyrights, trademarks, integrity.**

DOI: 10.18421/TEM121-63
https://doi.org/10.18421/TEM121-63

Corresponding author: *Khalid Kadhim Jabbar, Mustansiriyah University, Collage of Education, Computer Science Department, Baghdad-Iraq.* **Email:** khalidk.jabbar@uomustansiriyah.edu.iq

Received: 06 November 2022.
Revised: 17 December 2022.
Accepted: 10 February 2023.
Published: 27 February 2023.

1. Introduction

Web communities are places where people can meet up and share information have emerged due to digital communications and cheaper internet access. Online communities reflect our need for fast, straightforward communication. Facebook, MySpace, and Study are examples of the former, whereas DevianArt and Flickr are examples of the latter. No matter the online community, members share personal details, opinions on different media files, and other stuff. Multimedia file sharing provides both entertainment and information. How to protect others' creations online is a significant issue for the free exchange of ideas and material. Photos, songs, and movies may be uploaded to Facebook and shared in minutes. Even though their works are free, most writers demand recognition and payment for commercial use. Online authors lose control over how their works are distributed. It's possible for others to share your content online, or even steal it for their own commercial or promotional purposes. The intellectual property rights to the user-generated or linked content are claimed by social networks. Even while social networks typically have their own private legal and technological boundaries that restrict the sharing and reuse of data, unchecked diffusion and connection to intellectual property lead to two significant concerns. In the absence of a clear method of determining whether or not a work is in the public domain and free to use, many consumers may incorrectly conclude that they are free to do so. They could be sued if they're wrong, but they doubt it. Some internet users steal another's work and then try to sell it or claim ownership. True authors must prove authorship to assert their rights. Because works are often shared and with no records, this is challenging. To successfully address both challenges and increase legal compliance, a new technology strategy is needed that could change social networking culture and user behavior [1].

Our comparison aims to review picture encryption methods. These approaches are characterized by chaotic maps, DNA, DCT, GA, XOR operations, neural networks (NN), and optical image encryption.

2. Importance of IPR

Intellectual property rights are a standard for the growth and prosperity of society. IPRs empower creators to compete, which boosts society's growth. IP rights include: Protected IPR allows researchers and innovators to use previously unavailable materials without paying a fee, and it encourages creativity. These laws encourage novel works, products, and services. IP protection promotes economic growth. Intellectual property rights are vital to economic success. They foster honesty, which is crucial to economic and social success. Sustaining global economic growth needs efficient enforcement of IP rights. Damage IPRs were supposed to foster innovation and creativity by protecting their owners' interests, which would benefit society and humanity. IPRs are considered regressive since they give a few people power over resources. A few can stop vast efforts. Intellectual property rights are supposed to protect the public interest, but they really damage it.

3. Short History

IPR laws and administrative procedures have their origins in Europe. The practice of issuing patents began in the fourteenth century. In some ways, England was technologically advanced compared to other European countries, and it used to draw artisans from other countries on favorable terms. The first known copyrights were established in Italy. Venice can be considered the cradle of the IP system because it established the main rules in this area, where the laws and mechanisms were created for the first time in the world, and other countries followed suit in due course.

4. Role of Undisclosed Information in Intellectual Property

Although it is possibly the most significant kind of protection for enterprises, R&D institutions, and other organizations working with IPR, the protection of secret knowledge is the least well-known and least discussed aspect of intellectual property rights (IPR). Any secret recipe, compilation, program, device, method, technique, or process is considered a trade secret and is protected from public disclosure.

Humanity has always had mechanisms in place to prevent sensitive information from falling into the wrong hands, usually by keeping it within the intimate circle of family and friends. The pressure of globalization or internationalization were not intense from the 1950s to the 1980s; so many countries were able to get by without implementing a strong system of IPR. However, the laws relating to all forms of IPR are at varying stages of implementation [2].

5. Image Encryption

In many cases, images conceal sensitive information. The need to protect images from unauthorized access arises from the widespread use of images in sensitive areas, such as military communication, remote sensing, and medical imaging. As one of the most reliable means of data protection, encryption can facilitate this objective. The past several years have seen a proliferation of picture encryption techniques created by scientists. The images are encrypted using a variety of approaches to increase security. You can use encryption to store data safely and (ii) send sensitive information over the internet without worrying about anybody else reading it. As images become more widely used in various industries, including e-commerce, the military, medical, education, aerospace, and more, both are becoming increasingly crucial. Both the number and sophistication of assaults against networks are well-known to be on the rise [3],[4],[5].

6. Related Work Based On Encryption Techniques

The process of encrypting images is a good way to protect intellectual property rights by making it hard to get an image without the owner's permission. This is the goal of the current research, which will show the most important methods and techniques that have been reached and developed. In this field, although they are many and cannot be identified in one study, we have tried to collect the largest number of them. Because images are so useful in many fields, including military communication, remote sensing, and medical imaging, it is essential that private and sensitive information contained within them be safeguarded. In the existing research, several image encryption methods were categorized according to the primary encryption scheme applied throughout the encrypting process, and these primary schemes will be now briefly presented.

6.1. Chaos-based approaches

Image encryption based on chaos theory is widely used. The optimum features of chaotic systems are responsible for this plethora.
The goal of the system proposed in [6] is to provide users with a high degree of flexibility and ease of usage in managing change operations, accelerating encryption operations, intruding on the contents of message packets (various types and forms of sensor data) at the point of origin, and then decrypting and checking the integrity of the packets at the destination. These enhancements will increase users' confidence in one another. The proposed encryption mechanism was successful, as was the unique chaotic system. If you try to brute-force your way into the system's secret keys, you'll likely run into a wide range of permutations in the chaos key space that ensues. [7] To improve the quality of color images, we propose a nonlinear adaptive filter based on a model of chaotic amplitude, phase, and frequency (APFM). The APFM nonlinear adaptive filter is fed simulated time intervals, starting values, and nine parameters to generate randomness. Due to the nearly correct arrangement of the RGB components, a colored image can be encrypted into a cipher image. If you want to take colorful photographs, primary sensitivity is your best bet. According to NIST SP 800-22a, the proposed method is acceptable (cryptographic system secure tests). Data from the experiments demonstrates high safety. To develop a robust chaotic system, the authors of [8] combine two 1D chaotic maps (seed maps). This method can generate several 1D chaotic maps from their seed maps, each with larger chaotic ranges and more favorable chaotic attitudes, depending on performance evaluation and simulation outcomes. This method always starts with the same picture. Thereafter, it can create a one-of-a-kind encrypted picture.

6.2. Methods Based on Neural Networks (NN)

Dendrites integrate tens of thousands of temporal impulses. These signals convolute their own potential. This change is caused by synaptic stimulation or inhibition. A NN is highly parallelized and has the topology of a directed graph. Artificial neuron networks are used to depict NNs. Neuronal signal structures and functions affect group behavior. NNs are networks of neurons that can learn and adapt in parallel. [9] NN study was presented that summarized human-like behavior and features of the nervous system. In [10], a method for adding deep NNs into holomorphic encryption is updated. Authors focus on the CNN taxonomy (CNN).

A novel CNN method based on Tanh, ReLU, and Sigmoid activation functions. After testing the model's efficacy, these approximate activation functions are used. We apply CNNs on encrypted data and assess the model's performance. The sender utilizes holomorphic encryption to keep requirements secret, while the receiver uses a trained model to predict encrypted input. The model sends a prediction in the same code after deciphering a message. Only the data owner has access to the original data and expected value. Based on this research, secure NNs prediction services in the cloud can protect millions of customers' personal data. In [11], the proposed method focused on the well-known classification of convolutional neural networks (CNN) based on homogeneous coding schemes in order to develop novel techniques for solving deep neural network problems on encrypted input. [12] Encodes a hyper chaotic image using an autonomous deep feature extractor. The authors' method outperforms standard deep learning algorithms on face photo datasets. Image encryption is trending toward neural network-based approaches.

6.3. AES-based techniques

AES was invented by NIST in 1997. Rijndael is chosen as the AES algorithm [13] due to its superior mathematical soundness, rapid encryption, and safety, resistance to most attack types, and free use of copyright. AES-related papers are listed below. In 2011, scientists decrypted photos. Extra information is better hidden in pixel estimation errors before encoding than in encoded images. To calculate decryption error and bytes wasted, a comparative AES-based encryption technique is used. Key holders can see the original image. Hidden data can be implanted or recovered using the data hiding key. Error-free photo and data recovery trial results suggest the approach is effective and generally applicable (PSNR). Y. Qin et. al. [14] describes a cryptographic-stenographic method to restrict access to data. Steganography and encryption protect data. The suggested method in [15] includes AES-AQW photo encryption support, where an image that has been concealed is first turned into a mosaic, then encrypted with a key that is kept secret, and finally decrypted.

To do this, they used the AQW-connected quantum AES key stream generator. AES uses matrix singularities as keys. AES replaces Rcon with probability matrices. The AES algorithm's S-box and shift row mapping rules become corrupted with increasing clone probability distribution matrix size. Preprocessing employs a probability distribution matrix and plain-text XOR. [16]

Proposes a chaos-based random-key AES cryptosystem. It could improve encryption and key storage.

6.4. Methods Based on the RSA

RSA is an asymmetric cryptography algorithm. Asymmetric encryption requires a public and private key to work. A private key is confidential, while a public key is public. RSA was one of the first practical public-key cryptosystems and is used for secure data transfer. This cryptosystem makes the encryption key public while keeping the decryption key secret. Inability factor in the product of two large prime numbers causes this imbalance in RSA. An RSA user generates and distributes a public key with two large prime numbers and another value. Primes must be hidden. Everyone can encrypt with the public key, but decrypting requires the private key [17]. Images of varying sizes can be encrypted and decrypted with the new approach. The input image is first permuted with the help of a 1D Skew Tent map and a 1D Sin map; secondly, using the RSA encryption algorithm and a 3D logistic map, the result is encrypted; and finally, the result is permuted once again, a battery of tests on the proposed algorithm show that it has a large key space [18].

6.5. Techniques Relying on Pixel Values

The suggested method in [19], a teachable image encryption technique, this approach centers on the use of encrypted photos for network training, making it impossible for humans to view the images while they are being used for training. The network can be trained with no problems in this setup. The algorithm is validated using the Cifar dataset. Aradhana S. et. al. [20] makes some improvements to cryptography by using a new method that takes advantage of how pixels move. This approach both generates cipher pictures and recovers the original. After all, the algorithm encrypts and decrypts using RGB pixels. Digital image concealment with great precision is presented in [21].

6.6. Techniques Relying On The Least Significant Bit (LSB)

M. Tanaka in [22] has created smartphone software that uses LSB and AES to encrypt photographs and then hides them within another photo. For maximum safety, we utilize an AES key with a length of 256 bits. The Diffie-Hellman algorithm is used to secure the key against prying eyes. The Rapid Application Development (RAD) paradigm is used in this research as the project's development methodology. It allowed the process to cycle until a working application was achieved. By collecting requirements in this manner and allowing for early testing of prototypes during each iteration, significant issues can be mitigated before the application is released to the public. International Standards Organization/International Electro technical Commission/Institute of Electrical and Electronics Engineers Standard 29119 Testing standards are used to provide an interpretation of the application. In this analysis, we looked at the application's dependability, security, and usability. This leads to an improved overall performance evaluation.

6.7. Methods Based on (XOR) Operator

XOR (Exclusive OR) works like AND, OR, and NOT. This approach is safe. XOR is widely used in image processing. Below are some deviations. [23] Outlines the encryption and decryption operations; the starting image is displayed as a matrix and separated into equal-sized chunks (8 bytes). Here are several secret keys. Keys and blocks must have the same size and range (between 0 and 255). First, retrieve the encrypted color picture matrix, three-dimensional picture. It's a flat picture. The image matrix is divided into 8-byte pieces. Each private key can unlock eight elements. Each data blob is XOR with 4, 3, 2, and 1. Rearranging the encrypted data blocks reveals the original image. The research [24] covers two-stage steganography and cryptography using a sequential approach and symmetric XOR. The method described in [25] requires that the cover image contain a hidden message, its length, and its location within the cover image; it is acceptable to use key1 as the starting point for the message. Insertion assigns a single image byte to a text character.

6.8. Transformation-based image encryption

Transform-based methods of picture encryption involve mapping the input image to a different transform domain, such as frequency space. An R, G, and B color image is typically broken down into its component red, green, and blue channels (i.e., R, G, and B channels). Then, we use permutation and diffusion to encrypt each individual color channel. The color channels can be handled separately or jointly, depending on the situation. Channel encryption is followed by an inverse transformation to obtain the final encrypted image. Methods utilizing the transformed domain are explained below. Using no separable fractional ciphers, Ran et al. [26] came up with a method to solve the information-independence problem in picture encryption. For the purpose of secure data transmission, Fourier transform [27] created a method based on cascading FFT to encrypt multiple pictures.

Initially, the input photos are split into two distinct masks. The photos are encrypted using the second phase mask, which was generated using the first phase mask to generate the secret key. Image encryption based on modified Computational Integral Imaging Reconstruction was proposed by [28] as a solution to the occlusion problem in double-image encryption (CIIR). On the other hand, the transmission overhead of the network grows as more data is sent. Chen et al. [29] created double-image encryption based on the Gyrator Transform (GT) and a local pixel encryption technique. It provides insight into the phase-based imaging phenomenon of crosstalk dysfunction. In this method, two photos are blended to provide more sophisticated results.

6.9. DCT-Based Techniques

Image compression can be achieved with DCT. It's helpful in situations where a lot of pictures need to be kept in storage. Image quantization is the technique of dividing an image into discrete frequency components using a two-stage random matrix affine cipher that incorporates discrete wavelet processing. Y. Li et. al. in [30] present a new approach for encrypting and decrypting R, G, and B images. In contrast to other research that only discussed the keys used for picture encryption and decryption, the parameters and keys used in this form of encryption are arranged in a Random Matrix Affine Cipher (RMAC). A formula is constructed that selects keys for every feasible range, allowing for the encoding and decoding of R, G, and B images. Through simulation, the potential of the new approach has been examined. The outcomes demonstrate the efficiency and safety of using this approach with picture data.

6.10. Reversible Data Hiding

RLC allows the key generated by a linear feedback shift register to be used symmetrically in encipherment and decipherment processes [31]. Confidentiality is preserved along with reduced power consumption because of the usage with reversible logic [32], [33]. When comparing reversible logic to traditional binary logic, data preservation is improved [34], [35], [36]. Traditional methods like AES cryptography and others, on the other hand, offer less security and use more power [37]. A novel, reversible approach that can decrypt encrypted images is proposed in [38]. Confidentiality is achieved by encoding the actual image with an encryption key. Then, a single secret bit is used to embed every single block of the encoded image. The person who performs all of this behind the scenes with the help of the secret data-hiding key is known as the data hider.

Since data hiding operations are quite specific about which fractions of pixels should be flipped, even seemingly insignificant alterations to each block can have a significant impact on the final quality of the decrypted image. Hidden information in an encrypted image can be retrieved using a data-hiding key after the encrypted data has been decoded using a marked encryption key.

6.11. Techniques Based on Genetic Algorithms (GAs)

GAs are new to cryptography. Strong protection and fast-increasing bimolecular computation are in conformity with cryptographic requirements. Here are some GA-based papers. Public-key cryptography requires a key. Keys are categorized by fitness function to make GA a good alternative for key generation.

The proposed method in [39] suggests a GA-based technique for secure data transport and storage. DNA-Genetic Encryption Technique (D-GET) is recommended for increased security. This technique can turn digital data into DNA sequences and reshape, encrypt, cross-over, and mutate them, complete three D-GET cycles. Text or image files are transferred. At the receiving end, D-GET decrypts and reformats acceptable data. This approach converts text to image and vice versa. Safety is improved. Key sequences increase diffusion and misunderstanding. High-security ciphered information is difficult to decrypt. Experiments show that the suggested method offers many layers of defense against different types of attacks. The study [40] combines a Modified Genetic Algorithm with connected map lattices (MGA). This method uses a coupled map lattice to generate enough encrypted images for MGA. Second, MGA reduces the algorithm's computing time and increases the encrypted images' entropy.

6.12. DNA-Based Methods For Protecting Image Data

DNA cryptography's has many appealing features, including high throughput, large storage capacity, and negligible energy use, which led to its meteoric rise in popularity. Encoding and decoding are performed using the complementary laws of DNA [41].

The DNA-based image encryption mechanism is shown in block diagram form of Figure 1. Color images are often broken down into their component red (R), blue (B), and green (G) channels, starting with green (G). Following that, the channels are encoded using DNA encoding and XOR operations. Matrices are jumbled up using a chaotic map. The final step in obtaining the encrypted image is to merge the R, G, and B channels [42].

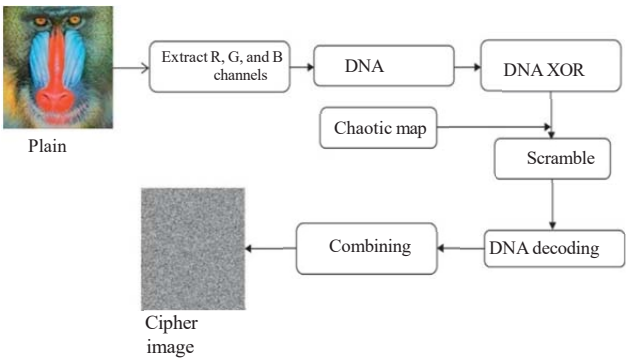

Figure 1 DNA based image encryption

6.13. Encrypting Photographs with an Elliptic Curve Algorithm

Small key sizes and low memory requirements are what make elliptic curve cryptography (ECC) so efficient [43]. **Figure 2** is an illustration of elliptic curve image encryption. It all starts with a grayscale conversion and compression of the original color image. After that, we encrypt using elliptic curves, the 3D Lorenz chaotic map, and the 4D Arnold cat map [44].

R. Guesmi et. al. [45], the researchers tried to come up with a way to use an elliptic curve to encrypt digital images. They used pseudorandom integers and substitution boxes to do this.

Elliptic curve ElGamal (EC-ElGamal) cryptography and chaotic theory were the basis for the asymmetric picture encryption method published by [46].

With the use of the ElGamal, a cryptosystem based on an elliptic curve analog, and the Mersenne Twister pseudorandom number generator, while [47] uncovered a method for encrypting medical images.

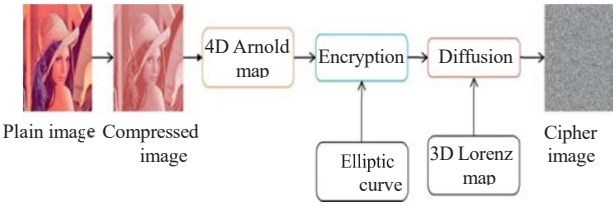

Figure 2 Encryption image using Chaotic map and elliptic

6.14. Cellular-automata-based image encryption

As a form of pseudorandom number generation, cellular automata have found widespread application in picture encryption. These models are somewhat involved, yet they are relatively efficient and reliable. Cellular automata rely on predefined rules to generate unpredictable outcomes.

Cellular automata have significance for cryptographic methods due to their parallelism, ease of implementation, and simple hardware structure [48]. The general architecture of cellular automata-based picture encryption is shown in **Figure 3.**

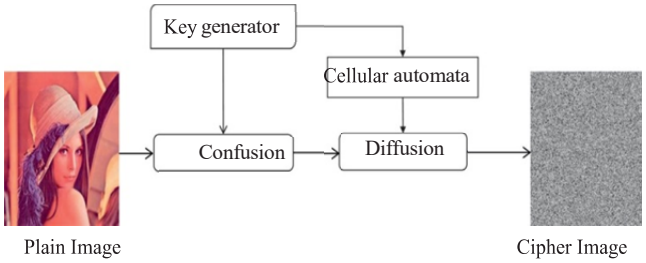

Figure 3 General framework of cellular automata based image encryption

The suggested method in [49], introduced a partial picture encryption approach. This cryptosystem has been proven to be invulnerable by a thorough security analysis.

6.15. Techniques for optical image encryption

Because of their fast computer speed and parallel processing capabilities, optical techniques are commonly used in cryptography.

To convert th original image into a stationary white noise representation, we employ Double Random-Phase Encoding (DRPE). In DRPE, randomized phase masks are critical. Y. Su et. al. [50] adopted number of optical encryption solutions based on nonlinear phase truncation after cylindrical diffraction and discrete wavelet transform, whereas [51] presented a scalable asymmetric image compression and encryption method (DWT). Y. Wang et. al. [52] Asymmetric multiple-image encryption was developed utilizing compressed sensing and phase truncation. To obtain a single cipher text, phase truncation is used following cylindrical diffraction. Y. Qin et al. [53] developed a phase-shortened, short-time fractional Fourier transform as well as hyper chaotic picture encryption. C. Wu. et. al. [54] used the phase-truncated Fresnel transform and a random amplitude mask to encrypt pictures (RAM). In [55], the researchers boosted processing speed and encryption capacity while decreasing iterations by using a chaotic map and a 2D straight canonical transform. [56], [57] To cipher an amplitude- and phase-truncated image, a gyrator wavelet transform was used. The proposed method is dependent on four variables: the level of the mother wavelet, the order of the gyrator transform, the position of the frequency bands, and the wavelet type. Variables use a secret key to encrypt photos.

[58] Nonlinear optical multi-image encryption was demonstrated. Using an enhanced amplitude-phase retrieval method.

7. Discussion And Analysis

Encryption technology is used to protect and secure images. Enormous has gone into making encryption more secure and sophisticated. These attempts can't be limited to one investigation, thus the current comparison. Multiple picture encryption methods exist. We've categorized picture encryption approaches as spatial, transformative, optical, and compressive. First, we categorized image encryption methods into three main groups based on general characteristics most methods share within one group.

Table 1 Methods analysis and comparison (Group-A)

Method	Advantages	Disadvantages
Chaos-based approaches	Guaranteed high security	-Not flexible -High size of memory -Higher latency -Difficulty to adapt to modern devices -High error propagation
Methods Based on Neural Networks (NN)	-Robust against various cryptanalysis (plaintext-only and chosen-plaintext attacks)	-Training RNNs - The vanishing or exploding gradient problem -RNNs cannot be stacked up -Slow and Complex training procedures -Difficult to process longer sequences
Techniques Based on Genetic Algorithms (GAs)	-strong protection.	-capacity for bimolecular computation is rapidly expanding
DNA-Based Methods For Protecting Image Data.	-Increase the algorithm complexity. -Cipher text unpredictability.	It is not suitable in the field of encryption, as it is better in the field of hiding information
Transformation-based image encryption: DCT, DWT, DFT, and FFT	-Very large key space. -Validity and the reliability. -Lower computational complexity. -Very high level of security.	It consumes time.

Then, we extracted the advantages and disadvantages of each group based on the results of most researchers in this field. Key Space Analysis (KA), Number of Pixel Change Rate (NPCR), Histogram Analysis (HA), Unified Average Changing Intensity (UACI), Information Entropy (IE), Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Execution Time (ET), Correlation Coefficient (CC), and Noise Attack were used to judge the quality of each method's results. Using the above criteria, we highlighted earlier approaches' most significant discoveries. Some techniques were marked with an (×) because they did not meet any of the evaluation criteria. We'll also designate strategies that have met the aforementioned requirements as (YES) or (NO) Based on the results and criteria of Tables 1, 2, 3, and 4, we created Table 5.

Table 2 Methods analysis and comparison (Group-B)

Method	Advantages	Disadvantages
AES, DES - based techniques	-AES provides encryption / decryption speed and security.	- very expensive - efficient for text encryption, need development to be efficient with image encryption
Methods Based on the RSA	- The RSA algorithm is simple to implement. -There is no need to worry about the security of your private data during transmission because the RSA method is used. -The mathematics involved in breaking the RSA method are extremely sophisticated, making cracking the algorithm a formidable challenge. - Distribution of the public key to users is simple.	As a result of the fact that RSA relies solely on asymmetric encryption, it is possible for it to fail in some circumstances where symmetric encryption would have been preferable. Due to the high volume of transactions, the data transfer rate is low. Sometimes a trusted third party is needed to validate public keys.
Techniques Relying on Pixel Values	Efficient for image encryption But it must be mixed with other techniques such as XOR, Chaotic system, ….etc.	It is affected by the type and nature of the image, and therefore the results will vary from one image to another.
Techniques Relying On The Least Significant Bit (LSB)	-Good quality of stego-image. -Higher level of security.	It can be applied in the spatial domain, but with the transform domain it may need to be a hybrid with an algorithm that has the ability to overcome the problem of changing the coefficient values.
Methods Based on Logic Gates	-Encryption of color, gray and binary images in an efficient way with higher security. -Limited resource utilization. - Efficient for image, and text encryption.	It can be implemented with all algorithms and does not change the results negatively if the encryption algorithm is successful.

Table 3 Methods analysis and comparison (Group-C)

Method	Advantages	Disadvantages
Reversible Data Hiding	In the field of hiding data inside the host, it may generate an image free of distortion, but it cannot be adopted in the field of encryption for a unit.	Need higher embedding capacity
Encrypting Photographs with an Elliptic Curve Algorithm	-Lossless and combined information hiding plans.	The elliptic curve discrete logarithm is the hard problem underpinning elliptic curve cryptography.
Cellular-automata-based image encryption	Provide Balance, correlation-immune, nonlinearity, and easy to implement in hardware.	Hard to implement in software.
Techniques for optical image encryption	-Dual layer of security. -Large key space of the encryption scheme to resist brute-force attacks.	consume time in encryption process

Table 4 Evaluation parameters of image encryption techniques.

Evaluation parameter	Methods		
	Group A	Group B	Group C
Key space analysis	More than 2^{100}	More than 2^{100}	Less than 2^{100}
Histogram analysis	Random distribution	Random distribution	NO
Information entropy	Equal to 8, for a 256-gray scale image	×	NO
Noise a ttack	NO	NO	NO
Correlation coefficient	YES	YES	NO
Mean squared error	YES	YES	YES
Peak signal-to-noise ratio	YES	YES	YES
Execution time	Consumed time	No consume time	Consumed time
Number of pixel change rate	×	×	×
Unified average changing intensity	×	×	×

Table 5 Property Comparison

Properties	Methods		
	Group A	Group B	Group C
Compression	YES	NO	YES
Loss	YES	NO	YES
Authentication	HIGH	HIGH	MIDDEL
Complexity	LOW	HIGH	HIGH
Randomness	HIGH	YES	MIDDEL
Consuming Time	YES	NO	YES
Integrity	NO	YES	NO
Memory Usage	HIGH	NO	HIGH

By reviewing the techniques that were used in the encryption process for images in the above tables, we noticed that the use of some techniques without improvements or auxiliary technical additions gave better results than the results we would get if we used the mentioned techniques individually. Moreover, we found that an important fact lies in logic gates that can contribute significantly to improving the performance of any method or technology that will be adopted in the encryption process because it will increase the length of the key, increase complexity, and prevent redundancy.

8. Conclusion

From the above table, we note that in group (A), most of the methods required pressure to complete the work, and therefore, the loss of part of the information in the image is certain. On the other hand, reliability is high due to complexity and average randomness. In addition to its consumption of time due to the complexity available in it, its consumption of a large area is possible; it is integrated if it is hybridized with powerful encryption algorithms. Group does not need to compress within its methodology, so losing information from the image is not an option. On the other hand, the reliability provided by the mentioned techniques is high due to their integration, as they can be used as an important part of the encryption process. The complexity in the design and implementation is not great, and it does not need complementary parts to complete its work.

The randomness is clear and achieved in the process of generating the key used in the encryption, which increases the chance of not repeating the process.

Furthermore, the techniques in Group A need a large amount of storage space because of their simplicity in design and implementation.

As for group (C), we have noticed the use of a set of accompanying techniques in order to complete the encryption process, and some of these techniques need to be compressed, so the loss of information is possible, the reliability is good, and the degree of complexity is high due to direct dealing with pixel values in the time domain or in the frequency domain.

The randomness is medium, and the probability of a successful encryption is low. However, key duplication is possible if one of the methods of key duplication is used. On the other hand, it takes more time to complete the encryption process and consumes more storage space.

Acknowledgements

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

Reference

[1]. Ilchev, S., & Ilcheva, Z. (2011, July). Protection of Intellectual Property in Web Communities by Modular Digital Watermarking. In *2011 IEEE 35th Annual Computer Software and Applications Conference Workshops* (374-379). IEEE.

[2]. Saha, C. N., & Bhattacharya, S. (2011). Intellectual property rights: An overview and implications in pharmaceutical industry. *Journal of Advanced Pharmaceutical Technology & Research, 2*(2), 88. Doi: 10.4103/2231-4040.82952.

[3]. 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 and Systems, 15*(2).

[4]. Mohammed, A. H., & Mahdi, A. M. (2021). A security services of proposed social web of things. *UPB Scientific Bulletin, Series C: Electrical Engineering and Computer Science*, *83*(4), 283-292.

[5]. Shibeeb, A. K., Ahmed, M. H., & Mohammed, A. H. (2021). A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation. *Karbala Int. J. Mod. Sci*, *7*, 175-188.

[6]. oomod, H. K., Naif, J. R., & Ahmed, I. S. (2020). A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system. *Periodicals of Engineering and Natural Sciences, 8*(4), 2333-2345.

[7]. Tong, X. J., Zhang, M., Wang, Z., Liu, Y., Xu, H., & Ma, J. (2015). A Fast Encryption Algorithm Of Color Image Based On Four-Dimensional Chaotic System. *Journal of Visual Communication and Image Representation, 3*(3), 219–234.

[8]. Hsiao, H. I., & Lee, J. (2015). Color Image Encryption Using Chaotic Nonlinear Adaptive Filter. *Signal Processing, 117*, 281–309.

[9]. Ismail, S. M., Said, L. A., Radwan, A. G., Madian, A. H., & Abu-ElYazeed, M. F. (2020). A novel image encryption system merging fractional-order edge detection and generalized chaotic maps. *Signal Processing*, *167*, 107280.

[10]. Isac, B., & Santhi, V. (2011). A study on digital image and video watermarking schemes using neural networks. *International Journal of Computer Applications*, *12*(9), 1-6.

[11]. Hesamifard, E., Takabi, H., & Ghasemi, M. (2017). Cryptodl: Deep neural networks over encrypted data. *arXiv preprint arXiv: 1711.05189.*

[12]. Xie, P., Bilenko, M., Finley, T., Gilad-Bachrach, R., Lauter, K., & Naehrig, M. (2014). Crypto-nets: Neural networks over encrypted data. *arXiv preprint arXiv:1412.6181*.

[13]. Li, X., Jiang, Y., Chen, M., & Li, F. (2018). Research on iris image encryption based on deep learning. *EURASIP Journal on Image and Video Processing*, *2018*(1), 1-10.

[14]. Qin, Y., Zhang, C., Liang, R., & Chen, M. (2019). Research on face image encryption based on deep learning. In IOP Conference Series: Earth and Environmental Science, 252. IOP Publishing.

[15]. Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption using advanced encryption standard. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *3*(3), 118-126.

[16]. Zhang, W., Ma, K., & Yu, N. (2014). Reversibility improved data hiding in encrypted images. *Signal Processing*, *94*, 118-127.

[17]. Joseph, M. (2015). Mosaic Image Steganography Based Color Transformation for Enhanced Security, *IJMTER, 2*(10), 149–156.

[18]. Liu, G., Li, W., Fan, X., Li, Z., Wang, Y., & Ma, H. (2022). An Image Encryption Algorithm Based on Discrete-Time Alternating Quantum Walk and Advanced Encryption Standard. *Entropy*, *24*(5), 608.

[19]. Abbas, E. A., Karam, T. A., & Abbas, A. K. (2019). Image cipher system based on RSA and chaotic maps. *Eurasian Journal of Mathematical and Computer Applications*, *7*(4), 4-17.

[20]. Sahoo, A., Mohanty, P., & Sethi, P. C. (2022). Image Encryption Using RSA Algorithm. In *Intelligent Systems: Proceedings of ICMIB 2021* (641-652). Singapore: Springer Nature Singapore.

[21]. Hamza, Y. A., & Omer, M. D. (2021). An Efficient Method of Image Encryption Using Rossler Chaotic System. *Academic Journal of Nawroz University*, *10*(2), 11-22.

[22]. Tanaka, M. (2018). Learnable Image Encryption. 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 1-2.

[23]. Kester, Q. A., & Koumadi, K. M. (2012). Cryptographie Technique For Image Encryption Based On The RGB Pixel Displacement. *IEEE 4th International Conference on Adaptive Science & Technology (ICAST)*, 74–77.

[24]. Li, X., Li, J., Li, B., & Yang, B. (2012). High-Fidelity Reversible Data Hiding Scheme Based On Pixel-Value-Ordering And Prediction-Error Expansion. *Signal Processing, 93*(1), 198–205.

[25] Tuieb, M.B., Mahmood, A.S., & Abbas, F.N., (2022),"Fusion of DWT as a Novel Approach for Efficient, Secured and Reversible Video Steganography", 2322(1), pp. 012093.

[26]. Al-Dwairi, M. O., Hendi, A., & AlQadi, Z. (2019). An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Image. Engineering, *Technology and Applied Science Research, 9*(3), 4165–4168.

[27]. Rasras, R. J., AlQadi, Z. A., & Sara, M. R. A. (2019). A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages. *Engineering, Technology and Applied Science Research, 9*(1), 3681–3684.

[28]. Gil, S. K. (2016). Asymmetric public key cryptography by using logic-based optical processing. *Journal of the Optical Society of Korea*, *20*(1), 55-63.

[29]. Ran, Q., Yuan, L., & Zhao, T. (2015). Image Encryption Based On NonSeparable Fractional Fourier Transform and Chaotic Map. *Optics Communications, 348*(1), 43–49.

[30]. Li, Y., Zhang, F., Li, Y., & Tao, R. (2015). Asymmetric Multiple Image Encryption Based On The Cascaded Fractional Fourier Transform. *Optics and Lasers in Engineering, 72*, 18–25.

[31]. Li, X. W., & Lee, I. K. (2015). Modified Computational Integral Imaging-Based Double Image Encryption Using Fractional Fourier Transform. *Optics and Lasers in Engineering, 66*, 112–121.

[32]. Chen, J. X., Zhu, Z. L., Fu, C., Zhang, L. B., & Yu, H. (2015), Analysis And Improvement Of A Double-Image Encryption Scheme Using Pixel Scrambling Technique In Gyrator Domains, *Optics and Lasers in Engineering, 66*, 1–9.

[33]. Sarala, B. et al. (2021). Efficient Design of Image Cipher Technique Using Reversible Logic. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(13), 691-700.

[34]. Cheng, C. S., Singh, A. K., & Gopal, L. (2015). Efficient Three Variables Reversible Logic Synthesis Using Mixed-Polarity Toffoli Gate. *Procedia Computer Science, 70*, 362–368.

[35]. Amrtha A. K., & Dheena K., (2016). Lossless And Reversible Data Hiding In Encrypted Images With Public Key Cryptography. Current Trends in Information Technology, 6(2), 27-33.

[36]. Rani, P. M. N., Kole, A., Datta, K., & Chakrabarty, A. (2016). Realization of ternary reversible circuits using improved gate library. *Procedia Computer Science, 93*, 153–160.

[37]. Xiang, S., & Luo, X. (2018). Reversible Data Hiding In Homomorphic Encrypted Domain By Mirroring Cipher Text Group. *IEEE Trans. Circuits Syst. Video Techno, 28*(11), 3099–3110.

[38]. Zhou, R., Shi, Y., & Cao, J. (2010). Transistor Realization Of Reversible Series Gates And Reversible Array Multiplier. *Microelectronics Journal, 42*(2), 305–315.

[39]. Zodpe, H., & Sapkal, A. (2018). An Efficient AES Implementation Using FPGA With Enhanced Security Features. *Journal of King Saud University - Engineering Sciences, 7*(2).

[40]. Chen, Y. C., Hung, T. H., Hsieh, S. H., & Shiu, C. W. (2019). A New Reversible Data Hiding In Encrypted Image Based On Multi-Secret Sharing And Lightweight Cryptographic Algorithms. *IEEE Transactions on Information Forensics and Security, 14*(12), 3332–3343.

[41]. Qin, C., & Zhang, X. (2015). Effective Reversible Data Hiding In Encrypted Image With Privacy Protection For Image Content. *Journal of Visual Communication and Image Representation, 31*, 154–164.

[42]. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F. G., & Coelho, V. N. (2018). Medical Image Encryption Using A Hybrid Model Of Modified Genetic Algorithm And Coupled Map Lattices. *Optics and Lasers in Engineering, 110*, 24.

[43]. Kuffi, E.A., Mehdi, S.A., Mansour, & E.A. (2022), Color Image Encryption Based on New Integral Transform SEE, *Journal of Physics, 2322*(1), pp. 012016.

[44]. Chai, X., Chen, Y., & Broyde, L. (2017). A Novel Chaos-Based Image Encryption Algorithm Using DNA Sequence Operations. *Optics and Lasers in Engineering, 88*, 197–213.

[45]. Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). A Novel Chaos-Based Image Encryption Using DNA Sequence Operation And Secure Hash Algorithm Sha-2. *Nonlinear Dynamics, 83*(3), 1123–1136.

[46]. Toughi, S., Fathi, M. H., & Sekhavat, Y. A. (2017). An Image Encryption Scheme Based On Elliptic Curve Pseudo Random And Advanced Encryption System. *Signal Processing, 141*, 217–227.

[47]. Wu, J., Liao, X., & Yang, B. (2017).Color Image Encryption Based On Chaotic Systems And Elliptic Curve Elgamal Scheme. *Signal Processing, 141*, 109–124.

[48]. Hayat, U., & Azam, N. A. (2019). A Novel Image Encryption Scheme Based On An Elliptic Curve. *Signal Processing, 155*, 391 402.

[49]. Zhang, W., Zhu, Z., & Yu, H. (2019). A Symmetric Image Encryption Algorithm Based On A Coupled Logistic-Bernoulli Map And Cellular Automata Diffusion Strategy. *Entropy, 21*(5), 504.

[50]. Su, Y., Wo, Y., & Han, G. (2019). Reversible Cellular Automata Image Encryption For Similarity Search. *Signal Processing, Image Communication, 72*, 134–147.

[51]. Ramírez Torres, M. T., Mejía Carlos, M., Murguía Ibarra, J. S., & Ontañon García, L. J. (2019). Partial Image Encryption Using Cellular Automata. *Computaci´on y Sistemas, 23*(4).

[52]. Wang, Y., Zhao, Y., Zhou, Q., & Lin, Z. (2018). Image Encryption Using Partitioned Cellular Automata. *Neurocomputing, 275*, 1318–1332.

[53]. Qin, Y., & Gong, Q. (2014). Multiple-Image Encryption In An Interference-Based Scheme By Lateral Shift Multiplexing. *Optics Communications, 315*, 220–225.

[54]. Wu, C., Hu, K. Y., Wang, Y., Wang, J., & Wang, Q. H. (2019). Scalable Asymmetric Image Encryption Based On Phase-Truncation In Cylindrical Diffraction Domain. *Optics Communications, 448*, 26–32.

[55]. Yu, S. S., Zhou, N. R., Gong, L. H., & Nie, Z. (2020). Optical Image Encryption Algorithm Based On Phase-Truncated Short-Time Fractional Fourier Transform And Hyper-Chaotic System. *Optics and Lasers in Engineering, 124*, 105816.

[56]. Chen, W. (2016). Optical multiple-image encryption using three-dimensional space. *IEEE Photonics Journal*, *8*(2), 1-8.

[57]. Huang, Z. J., Cheng, S., Gong, L. H., & Zhou, N. R. (2020). Nonlinear Optical Multi-Image Encryption Scheme With Two-Dimensional Linear Canonical Transform. *Optics and Lasers in Engineering, 124*, 105821.

[58]. Wu, C., Wang, Y., Chen, Y., Wang, J., & Wang, Q. H. (2019). Asymmetric Encryption Of Multiple-Image Based On Compressed Sensing And Phase-Truncation In Cylindrical Diffraction Domain. *Optics Communications, 431*, 203–209.