




Review

Medical Image Encryption: A Comprehensive Review

Saja Theab Ahmed ^{1,*}, Dalal Abdulmohsin Hammood ¹, Raad Farhood Chisab ², Ali Al-Naji ^{1,3,*}
and Javaan Chahl ³

¹ Electrical Engineering Technical College, Middle Technical University, Baghdad 10022, Iraq; dalal.hammood@mtu.edu.iq

² Technical Institute Kut, Middle Technical University, Kut 52001, Iraq; raadfarhood@yahoo.com

³ School of Engineering, University of South Australia, Adelaide, SA 5095, Australia; javaan.chahl@unisa.edu.au

* Correspondence: bbc0070@mtu.edu.iq (S.T.A.); ali_al_naji@mtu.edu.iq (A.A.-N.)

Abstract: In medical information systems, image data can be considered crucial information. As imaging technology and methods for analyzing medical images advance, there will be a greater wealth of data available for study. Hence, protecting those images is essential. Image encryption methods are crucial in multimedia applications for ensuring the security and authenticity of digital images. Recently, the encryption of medical images has garnered significant attention from academics due to concerns about the safety of medical communication. Advanced approaches, such as e-health, smart health, and telemedicine applications, are employed in the medical profession. This has highlighted the issue that medical images are often produced and shared online, necessitating protection against unauthorized use.

Keywords: medical image encryption; security; E-healthcare; chaotic map; ECC; DNA; PQC; lightweight cryptography



Citation: Ahmed, S.T.; Hammood, D.A.; Chisab, R.F.; Al-Naji, A.; Chahl, J. Medical Image Encryption: A Comprehensive Review. *Computers* **2023**, *12*, 160. <https://doi.org/10.3390/computers12080160>

Academic Editor: Paolo Bellavista

Received: 20 July 2023

Revised: 3 August 2023

Accepted: 8 August 2023

Published: 11 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Electronic health records (EHRs) are a type of digital health record that is regularly created, updated, and disseminated online to facilitate efficient, accurate data collection thanks to the proliferation of smart and intelligent technologies [1,2]. A patient's electronic health record is a collection of data about the patient maintained by the relevant healthcare providers, including the patient's demographics, medical history, symptoms, and other relevant data. Images sent over the internet are vulnerable to eavesdropping, tampering, unauthorized duplication, and other forms of theft because they are sent in clear text. With today's heavy reliance on electronic communication networks, protecting private information is more important than ever [3]. In light of this, there has been an increased focus in recent years on protecting the image in an effective manner. The fundamental concept is to encrypt these images with an algorithm so that an adversary cannot decipher any salient data. The techniques are extremely sensitive to changes in starting point, parameters used for control, periods, ergodicity, and even the appearance of randomness. The term "cryptography" refers to either the practice of encrypting data or the study of how such data is encrypted [4]. Before being transmitted via public networks, the actual data are first transformed into a representation that is meaningless without additional information. One of the most frequently suggested methods for ensuring the safety of medical images in the healthcare industry is encryption [5]. In this plan, the original image is transformed into a cipher image, and only authorized users are able to view its contents [6]. This prevents unauthorized users from gaining access to the data. Cryptography is frequently employed now because of the considerable security benefits it provides. The numerous motivations behind the use of cryptography are listed below in Figure 1. In general, there are two main categories that can be used to categorize encryption methods: symmetric and

asymmetric procedures. To secure an image using symmetric encryption, it is essential to maintain a singular key. Conversely, the utilization of asymmetric techniques necessitates the preservation of two distinct keys [6]. Figure 2 shows the basic procedure for medical image encryption.



Figure 1. The motivations for the use of cryptography.

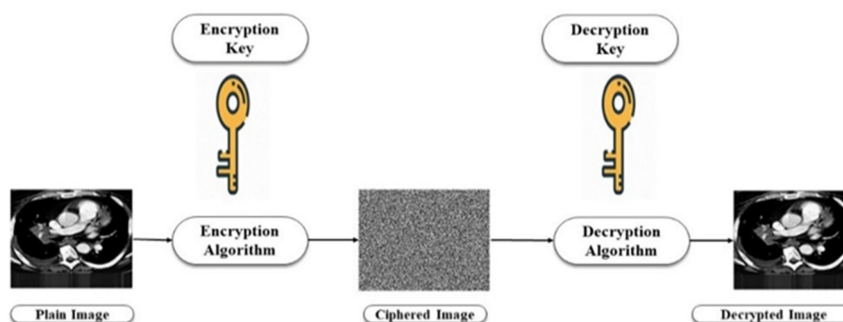


Figure 2. The basic procedure for medical image encryption and decryption.

Asymmetric encryption is superior to symmetric encryption but more time-consuming to implement [1]. Over the last few decades, academics have relied on traditional encryption methods to guarantee the authenticity of images. Due to the inherently different characteristics of digital images, however, it is no longer possible to put these ideas into effect [7]. The efficient encryption system was created by researchers as a solution to the problem of medical image confidentiality. To that end, this article's primary contribution is a primer on the history and evaluation metrics of picture encryption. Then, we discuss the benefits and drawbacks of several medical image encryption systems. In addition, the estimated design objectives, targets, methodologies, assessment measures, and weaknesses are outlined with the contributions of the surveyed scheme. Finally, contemporary challenges are underscored, and numerous avenues of potential research that may contribute to bridging the existing gaps in these domains are highlighted, thereby facilitating the endeavors of academics and developers alike. To protect sensitive information and prevent unauthorized changes, cryptography offers a variety of safeguards.

The following is how the paper is organized: In Section 2, we covered why it is necessary to encrypt medical images. We have outlined what is required for image encryption methods in Section 3. We introduced the measurements and criteria used to compare the

effectiveness of different encryption algorithms in Section 4. In Section 5, we talk about a few common attacks in the domain of image processing.

Also, we have given a literature study and classification of the most common image encryption schemes In Section 6. Section 7 includes the cryptographic systems and components. The conclusion is discussed in the final section.

2. The Purpose of Encrypting Medical Images

The encryption of medical images is a growing area of application for cryptographic systems, and as such, it should be performed using efficient algorithms that require low cost and time. When encrypting an image, it is necessary to apply either a symmetric or an asymmetric encryption technique for the input image to be transformed into a cipher image utilizing either symmetric or asymmetric keys. This process is known as image encryption. Varying methods with different parameters can be used to encrypt medical images. The encryption of medical images can be accomplished by various methods, including high-speed scrambling [8], bitwise XOR diffusion, chaotic and edge maps, and so on. There are several ways to evaluate the effectiveness of the algorithm used to encrypt medical images, including the peak signal-to-noise ratio, the bit error rate, the fidelity, and the mean square error. Telemedicine, telesurgery, and teleradiology are examples of highly developed technologies that are currently undergoing the clinical trial and implementation phase. There is a risk that sensitive patient data will be transmitted across a network using these technologies. In particular, medical imaging (MRI, CT, and X-ray) are vulnerable to manipulation because of its vast data storage, redundancy, and strong pixel correlation. The development of a high-performance, efficient method of encrypting medical images is essential to:

- Confidential and secure communication of patients' medical records;
- Integrity Assurance;
- Preventing alterations to medical images that could cause a misdiagnosis;
- Avoid falling victim to cyber-attacks.

3. Requirements for Image Encryption

Due to the unique qualities of images, maintaining image security has evolved into a difficult challenge [9]. Guidelines for basic image encryption are shown in Figure 3. A number of the most important aspects of image encryption for privacy protection are outlined here.

- Security: An essential feature of any effective encryption method is a focus on security. To guarantee an image feature's trustworthiness, a separate encryption procedure should be used. In general, it involves elements of perceptual safety, key sensitivity, and resistance to possible threats.
- Perceptual security: When an encrypted image is produced as a result of an encryption process in such a way that it cannot be perceptually recognized, we say that the process is secure in perception.
- Keyspace: In cryptography, the term "key space" refers to all potential encryption keys that can be used during encoding. A larger key space value is preferable in terms of protection against exhaustive search attacks.
- Key sensitivity: What this means in practice is how much a change of just one bit in the encryption key will alter the cipher images. Every encryption method should be highly sensitive to private encryption key variation.
- Potential attacks: An ideal image encryption approach would be impervious to the various attacks that may be launched against the underlying cryptosystem, including ciphertext-only attacks, known-plaintext attacks, differential attacks, and so on.
- Computational complexity: Using a cryptographic model to encrypt all of a picture's data would result in an extremely high computational complexity for the entire image; hence only the most crucial data should be encrypted for security.

- Invariance of compression ratio: Invariance in the compression ratio of the encrypted image is necessary for the preservation of storage space, data transfer rates, and image quality after decompression.
- Real-time demand: Real-time performance can be seen in things like video conferencing and image surveillance, for example. A necessary requirement for encryption and decryption is to maintain a tolerable delay.
- Multiple levels of security: Various iterations and a range of key sizes can be utilized to keep security at a high level while also allowing for expansion.
- Transmission error tolerance: Real-time data transfer happens across noisy media. This suggests that an ideal for a flawless model of encryption is needed.



Figure 3. Basic guidelines of image encryption.

4. Image Encryption: An Evaluation and Assessment

In order to evaluate the efficacy of various encryption methods, many metrics and criteria are employed [10]. The following section will review some of the most common metrics, as shown in Table 1.

1. Visual assessment: Deciphering encrypted images requires a visual inspection of the binary, grayscale, and color versions of the image.
2. Statistical Analysis: Statistical analysis refers to the process of analyzing the correlations between the pixels of an encoded image. This evaluation makes use of the histogram and the correlation coefficient.
3. Differential Analysis: Finding out how a single bit shift in the secret key or a single pixel shift in the plain image affects the cipher image.
4. Security Analysis: We consider the following elements in our examination of the safety of every procedure:

- a. Key sensitivity analysis, or KSA: It evaluates the effect of a single-bit shift in the encryption key on the resulting encoded image. Pixel-by-pixel, two encrypted images are compared to reach a verdict.
 - b. Key Space Analysis: This examination is crucial to the viability of any encryption method in the face of brute-force attacks.
5. Time Complexity Analysis: Amount of time needed to carry out a set of commands. Consider the time needed to encrypt and decrypt an image. Its worth is conditional on a number of variables, such as the specific configuration of the system and the image format being employed.

Table 1. Standardized image encryption metrics.

Criteria for Evaluation	Description	Metric
Security	Any method of encryption that is unaffected by any possible risks.	Protecting against attacks while maintaining the appearance of vast key space and highly sensitive keys is essential.
Computational time	It is vital to compress images without losing quality to lessen the amount of space required for image storage or the bandwidth required for image transmission.	Uses the permutation and diffusion functions. The complexity and time required for encrypting and decrypting an image are extremely low.
Compression ratio	A size decrease is accomplished by compressing methods. It is the ratio between the uncompressed and compressed versions of the image.	Histogram analysis, correlation coefficient (CC), Number of Pixels Changed per Second (NPCR), Unified Average of Changing Intensity (UACI).
Robustness Quality	It is an examination of the difference in quality between the plain images and the decrypted ones.	Peak signal-to-noise ratio (PSNR), Structural Similarity Index (SSIM).
Entropy [11]	It is used to test the degree of randomness in cipher images.	$H(S) = -\sum_s(P(S_i) \times \log P(S_i))$.

5. Prevalent Forms of Image Attacks

In this section, a discussion is presented regarding several prevalent attacks encountered within the field of image processing [12,13].

1. Ciphertext-only: During this type of attack, cryptanalysts are only able to obtain access to certain groups of cipher texts; hence, they attempt to decrypt ciphertext in order to gain access to the secret key or plain text.
2. Known-plaintext: An attacker who has access to both the plaintext and the encrypted version of a message launches this kind of attack in an attempt to deduce the secret key used for the encryption.
3. Chosen-plaintext: A random plain image is chosen by the attacker and inserted into the encryption algorithm, allowing for a more thorough analysis of the related cipher image.
4. Brute-force: In order to decipher the data that has been encrypted, every conceivable combination of keys will be tried until the secret key can be discovered.
5. Differential attack: It is used to determine how sensitive an encryption method is to slight modifications to the original picture. The plain image is modified slightly by the attacker, who then uses the same encryption technique to encrypt both the original and modified versions of the image to determine how the original plain image compares to the encrypted image.
6. Noise: An attacker's goal here is to corrupt the useable information of the plain image by introducing noise into the encrypted image. If the intended recipient cannot restore the original image following decryption, the attack has succeeded.
7. Occlusion: Using this method, we can see how well we do at recovering lost data from encoded images that were compromised by hackers or just lost their connection to the internet.

8. Entropy: In this technique, the attacker creates “stale” packets by combining “fresh” packets from a later time period with “old” packets from a previous collection or interception. The system’s information entropy will decrease dramatically as a result of these packets’ lack of additional coding information.
9. Side channel attacks (SCAs): The use of Side-Channel Attacks, also known as SCAs, has become an efficient method for getting confidential information from cryptographic devices, which poses a significant risk to the devices’ level of security. Kocher introduces the concept of a side channel attack in the form of a timing assault, where an attacker monitors how long it takes a device to carry out a series of calculations and uses that data to learn more about the crypto-system [14]. He also has demonstrated that the key can be revealed through the cipher’s non-constant execution duration. A side-channel attack, in general, is a case where we have a security algorithm such as encryption, inputs and outputs, and a key that is super secure, and nobody is able to know that key. The entire security of the algorithm relies on this, or it is designed to protect that key. An adversary can gather information by monitoring the system’s power consumption, electromagnetic field (EMF), computation time, and memory access patterns rather than plaintext or ciphertext messages while it manipulates data. The attacker then looks into the relationships between the signatures observed in the side channel and the signatures predicted from the intermediate data and computation states. Private information may be leaked or made public as a result of this procedure. There are two distinct types of SCAs, namely profiled and nonprofiled assessments [15]. There are two stages to a profiled SCA: the profiling phase, during which an adversary is given a training device to test, allowing him to characterize physical leakages and obtain a precise leakage model, and the online exploitation phase, during which an attack is mounted against a similar target device in order to extract the secret key. SCA is shown in Figure 4 [16].

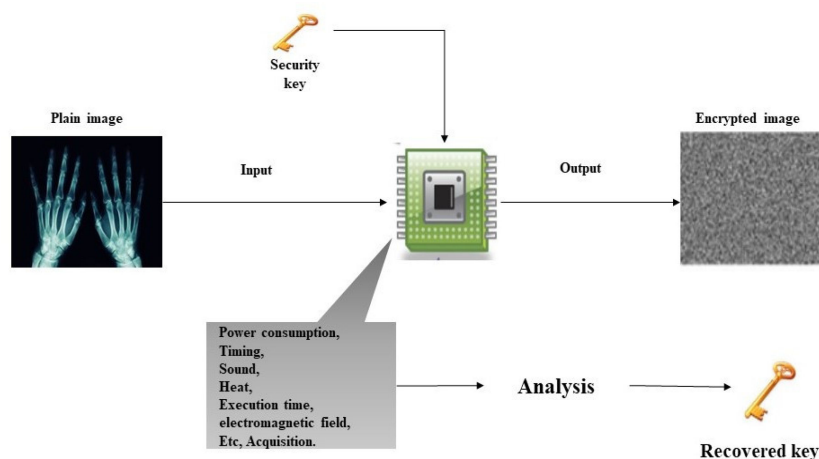


Figure 4. How Side-Channel Analysis Works.

Power analysis attacks (PAAs) are the most efficient type of SCAs since they are simple to execute in a test environment and require a low cost on the part of the attacker. PAAs are based on a power analysis calculation [17]. The main types of PAAs are:

- Simple power analysis (SPA): attempts to extract information about the functioning of a gadget by analyzing the amount of power that it consumes.
- Differential power analysis (DPA): plans to make use of the data dependencies that are present in the power usage pattern.
- Correlation power analysis (CPA): Using the hamming weight power model in CPA allows one to determine whether or not there is a correlation between the anticipated output and the actual power output of an encoded device [18].

10. **Fault Attack:** a fault analysis (FA) is a common and robust active SCA approach in which a defect inserted within the processes of a cipher may cause an error based on the parameters of internal secret states. Specifically, we classify fault attacks as either safe-error-based, weak-curve-based, or differential-fault-based. The idea behind “safe-error attacks” is that it is possible to make mistakes without significantly altering the outcome. In an effort to break a system, weak curve attacks convert scalar multiplications from strong curves to weak ones. Bit-by-bit scalar data can be retrieved by differential fault attacks by comparing the expected and unexpected output. In order to execute a fault attack, the attacker must have direct control over the victim’s device and must subject it to extreme external stress. Mean to cause faults in such a way that these errors result in a security fault in the system; in fact, in the fault attacks, we are facing some intentional alterations to expose the device to some out-of-specification physical conditions, such as high or low temperature and radiation [19]. On the other hand, an attack that is software-induced and causes a physical defect is also a possibility. Differential fault analysis (DFA) examines the information flow within the context of an implemented encryption [20].

Countermeasures for Power and Fault Analysis:

Employing diverse countermeasures that give protection against both power and fault attacks is the first step toward mitigating the effects of power and fault analysis, which is one of the possible solutions. Ref. [21] uses hardware redundancy and randomized cipher operations to thwart power analysis and cryptographic faults. It also utilizes fault space transformation (FST), in which redundant state computations are performed in different domains, making it challenging to induce the same error in redundant states. By rearranging the order of computations, a cipher makes it more difficult for an attacker to align the power traces of its internal processes. There is also an examination of how error detection using parity and hardware redundancy interact [22]. Both fault detection countermeasure types were found to significantly accelerate the rate of key recovery with CPA. In [23], data path shuffling is used to defend an AES implementation from localized EM fault attacks. One of the significant drawbacks of using different defenses against power and fault analysis is that defenses against one form of attack may have an unintended detrimental effect on defenses against the other sort of attack if they are not correctly built. Using concurrent error detection (CED) codes for fault protection has been proved in multiple studies to improve the accuracy of the power quality analysis [24].

In order to analyze an image, an evaluation of the image’s ciphering must be performed. Several metrics, summarized in Table 2, will be used in the evaluative process.

Table 2. Image encryption evaluation procedure.

Metric	Characterizations	Equations	Outlines
Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI) [25,26]	Evaluation of the Current Encryption Method NPCR’s range is 0 to 1. NPCR = 1 is ideally suited. A UACI of ≈34 is optimal for a 512 × 512 pixel image.	$D(i, j) = \begin{cases} 0, & \text{if } C1(i, j) = C2(i, j) \\ 1, & \text{if } C1(i, j) \neq C2(i, j) \end{cases}$ <p>NPCR:</p> $N(C^1, C^2) = \sum_{ij} \frac{D(i, j)}{T} \times 100\%$ <p>UACI:</p> $U(C^1, C^2) = \sum_{ij} \frac{ C^1(i, j) - C^2(i, j) }{F.T} \times 100\%$ <p>where, C^1 and C^2 are encoded images both before and after a single pixel change was made, L is the highest pixel value that can be supported, and T would be the complete number of pixels.</p>	It is essential for any cryptographic algorithm to have a NPCR ≥ 0.9, and UACI ≈ 0.33

Table 2. Cont.

Metric	Characterizations	Equations	Outlines
Correlation Coefficient (CC)	It characterizes the connection between the unencoded and encoded image's correlated pixels. The horizontal, diagonal, and vertical components are all taken into account. The CC scale goes from minus one to plus one.	$CC(x,y) = \sum \frac{c(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$ Here, $C(x,y) = \frac{\sum_{i=1}^k (x_i - E(x))(y_i - E(y))}{P}$ $D(x) = \frac{1}{p} \sum_{p=0}^n (x_i - E(x))^2$ $D(y) = \frac{1}{p} \sum_{p=1}^n (y_i - E(y))^2$ For which $E(x)$, $E(y)$, $D(x)$, $D(y)$ are the means and standard deviations of x and y , respectively. The covariance between x and y is denoted by $C(x,y)$, where p is the total number of pixel pairings (x_i, y_i) .	The CC value for an encrypted image should be ≈ 0
Mean Squared Error (MSE)	Validation of error values that establish the distinction between an encrypted image and a plain image MSE's range is 0 to ∞ .	$MSE = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \frac{[x(i,j) - y(i,j)]^2}{m} \times n$ where X and Y are the encrypted and unencrypted versions of the image, respectively. Pixels with coordinates (i, j) in an image of size $m \times n$.	Images with a low MSE are considered to be of high quality.
Peak Signal to Noise Ratio (PSNR)	Comparison of the quality of the plain images and the encrypted versions. The Range of PSNR is expressed as a number of decibels (dB) which is from 0 to ∞ .	$PSNR = \frac{10 \log_{10}(2n-1)^2}{MSE}$ where n is the number of bits per pixel.	The PSNR value between the original image and the decrypted images needs to be high.
Structural Similarity Index (SSIM)	Used for calculating the degree of similarity between the plain photos and the decrypted versions of those images. It's a metric used to rate the quality of the decrypted image. The spectrum of the SSIM: -1 to +1.	$SSIM = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$ Where (μ_x, μ_y) indicate the average and (σ_x^2, σ_y^2) indicate the variance of an input x and decrypted y images, respectively. σ_{xy} represent the covariance of x and y . c_1 and c_2 are regularization constant.	It should be for an exact duplicate of the image ≈ 1 .
Information Entropy (IE)	It is the average amount of data contained in a single pixel of an image. Values vary from pixel to pixel. IE range: 0 to +8.	$H(S) = -\sum_s (P(S_i) \times \log P(S_i))$ In which $P(S_i)$ is the possibility that S_i will show up in message source (S).	For an 8-bit image, the IE value needs to be closer to 8.
Execution Time (ET)	It specifies how long an image-encryption procedure takes to carry out. It is the sum of the compile and run times. ms, secs, and mins are the units of measurement.	-	ET should have less of an impact on the value of any encryption scheme.

6. Techniques of Image Encryption: A Literature Review

This section presents a taxonomy of image encryption techniques. Compressive sensing, optical encryption, spatial encryption, and transform domain encryption are the four primary categories that are used to classify image encryption techniques. Various methods of encrypting images are categorized in Figure 5. Several cryptographic processes can be used to ensure that medical images are transferred securely and cannot be intercepted [27].

As a result of their widespread popularity, the three methods employed in this paper because they are achieving the following goals in the field of medical image encryption:

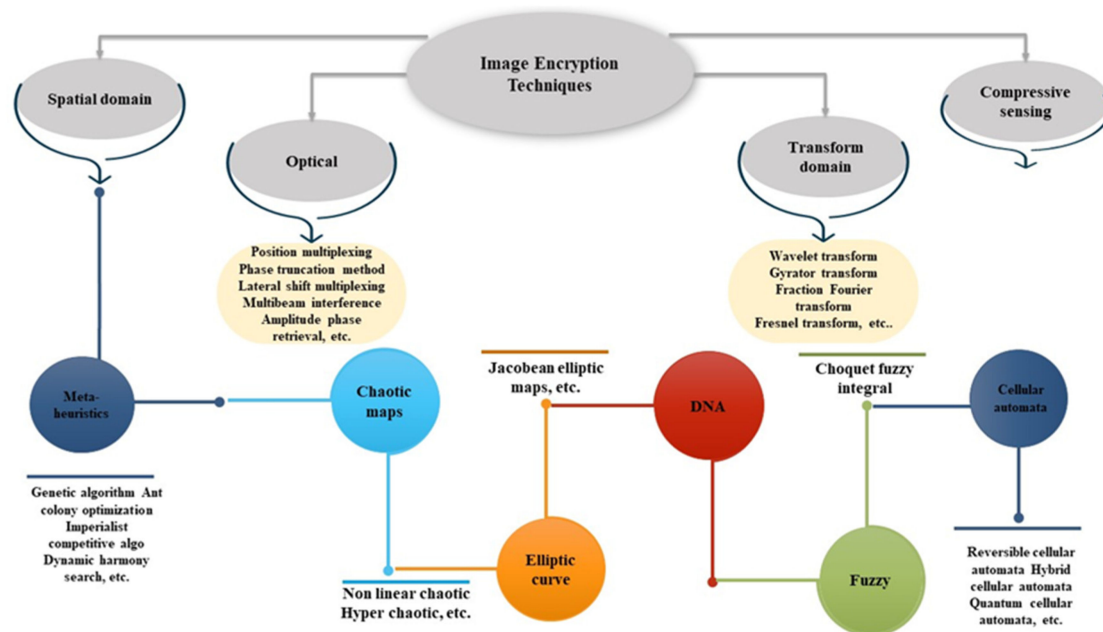


Figure 5. A taxonomy of image encryption techniques.

For chaotic maps:

- **Safety:** According to the theory of chaos, the state of a chaotic system can change drastically depending on its initial conditions. Encryption algorithms with high resilience to attacks can be designed by making use of this unpredictability and complexity. In order to improve the security of the encryption process, chaos-based encryption methods seek to utilize the chaotic behavior of mathematical models to either produce encryption keys or directly change the medical imaging data.
- **Nonlinearity:** Medical photos frequently feature complex structures and patterns that might be difficult to encrypt using linear methods. The nonlinear approach provided by chaos-based encryption algorithms makes it possible to encrypt medical image information in a more safe and reliable fashion. Complexity can be introduced by the chaotic dynamics, making it more difficult for an adversary to decipher the encryption.
- **Resistance to Statistical Attacks:** Healthcare images frequently display statistical regularities or patterns that could be used maliciously. To protect its encrypted data from statistical attacks, chaos-based encryption techniques might inject a large amount of unpredictability.

For ECC:

- **Key Size Efficiency:** ECC provides the same or more security than other encryption methods like RSA but with more manageable key sizes. This is helpful for protecting medical photos, which often measure in gigabytes and require speedy encryption and decryption procedures. ECC is a useful option for protecting medical images since its smaller key sizes allow for faster computations, and less storage space is needed.
- **Scalability:** It is common for medical imaging equipment to require the transmission and storage of several images. With ECC encryption methods, massive datasets can be encrypted and decrypted quickly and efficiently, allowing for scalability. ECC's faster computations and reduced key sizes make it possible to encrypt and handle large numbers of medical images without compromising security.
- **Regulatory Compliance:** HIPAA (Health Insurance Portability and Accountability Act) compliance is essential in the healthcare sector because of the sensitive nature

of patient information. Several government agencies have acknowledged ECC as a secure encryption method. When used to encrypt medical images, it aids institutions in fulfilling regulatory mandates for keeping patient information secure.

For DNA:

There are various potential motives and benefits for adopting DNA encryption techniques in medical image encryption:

- **Security:** Due to the unique properties of DNA, methods of DNA encryption can provide high levels of security. DNA-based encryption methods use the randomness and complexity of DNA sequences to encrypt and decrypt data. This protects the confidentiality of the patient's information by making it incredibly challenging for hackers to crack the encryption on medical photos.
- **Scalability:** DNA has a huge storage capacity, enabling the compact storage of massive amounts of data, such as medical images. Because of their potential size, high-resolution medical images benefit greatly from this scalability's encryption protection. The secure storing and encryption of massive volumes of visual data is a breeze for DNA-based encryption technologies.
- **Robustness:** DNA is a robust medium for long-term data storage since it is unchanging and resistant to external influences. DNA encryption technologies can protect the quality and endurance of encrypted data, making them ideal for archiving medical imaging for long periods of time.
- **Biocompatibility:** DNA encryption techniques are excellent for medical applications since they are compatible with living systems. DNA-based encryption techniques, for instance, can provide a biocompatible and non-toxic solution for the safe transmission and storage of medical pictures within the human body.
- **Emerging Technology:** DNA-based encryption techniques are an innovative and cutting-edge approach to data security. Researchers and practitioners in the field of medical image encryption can push the boundaries of the discipline and make significant contributions to the development of both encryption and medical imaging by incorporating such technologies.

DNA encryption technologies are still in the experimental stages of development and application. Although they hold promise for the future, additional research and development are necessary to completely comprehend their potential benefits and challenges in the context of medical image encryption.

For PQC

One of the key reasons for opting for Post-Quantum Cryptography (PQC) encryption methods is the expectation that quantum computers may one day be developed. Classical computers process and store information using binary digits (bits), but quantum computers employ quantum bits (qubits), which can be in more than one state at once. For some mathematical problems, such as those at the heart of many popular encryption techniques, quantum computers may be able to find solutions significantly more quickly than classical ones, thanks to their intrinsic parallelism. Researchers and security experts have been investigating and creating PQC encryption ways to counteract this immediate danger. PQC methods are designed to protect data in the long term from being compromised by either classical or quantum computers. These algorithms are built to withstand attacks from quantum computers, lowering our vulnerability to potential quantum computing developments in the future.

As a result of this, there is a heightened interest in learning more about these methods.

6.1. Encryption Based on Chaotic Maps

Given their behavior, chaotic maps are of particular interest in dynamic systems. This means that even a seemingly minor shift in the inputs might have a significant impact on the results. There are two main types, called discrete and continuous, respectively. Because of their advantageous balance of security and processing speed, chaotic maps see

widespread use in various communication scenarios [28]. Figure 6 represents the chaotic image encrypting process [29].

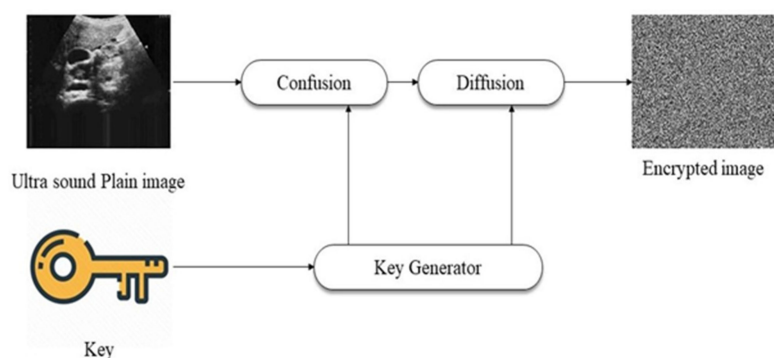


Figure 6. The encryption of images using chaotic maps [29].

The author in [30] used a method for the double encryption of images that was based on chaos to provide high security. The first step was encrypting the face extracted from the image, and the second encryption of the entire image. 2D SFSIMM (Two-dimensional hyperchaotic map, sinusoidal feedback Sine ICMIC modulation map) is responsible for generating the keystream for the cryptosystem. At the same time, both scrambling and diffusion were proposed. This technique is robust against various statistical attacks since the attacker needs to crack two rounds of the encryption algorithm.

In [31], to encode and decode images securely, a new cryptosystem based on three maps has been developed. The sine map is used in the permutation technique to adjust the coordinates of the pixels in the source image, while the substitution is performed on the permuted image using the second secret key K . Lastly, the CTM-based image scrambling is performed with a bit XOR.

A developed technique for chaotic image encryption using Latin squares and random shifts was suggested in [32]. Four steps comprise the algorithm: creating a key, scrambling pixels, swapping out pixels, and scrambling bits. The security and robustness of the procedure are both improved by increasing the resulting Latin square matrix's complexity. In order to increase the high sensitivity of the cryptography approach, the key is first produced from the plain image. The second step in achieving pixel position scrambling is to cyclically shift each pixel to the right within each row of the image matrix. Then, the image matrix's coordinate elements are replaced by the results of a lookup table comprised of a 256-by-256 Latin square matrix containing a chaotic sequence, with replacement coordinates determined depending on the values of the image's pixels and the sequence's values. The implementation of a multimedia encryption technique is difficult since it takes more resources (time and storage). Due to this, the lightweight image encryption technique, which uses minimal memory, time, or energy and offers the highest level of security for low-powered devices, is becoming more and more popular.

Therefore, a study by Ferdush et al. [33] studied the lightweight image encryption approach that was based on chaos. As a first step, the author developed a standardized approach and method for lightweight image cryptography based on two different chaotic maps, specifically Arnold and Logistic.

Another study [34] discussed the modification of pixel values and positions based on the SCAN algorithm and chaotic theory. The SCAN method includes converting the pixel value of an image to a new pixel value and then rearranging the pixels in the image in a specific order. Meanwhile, within the block, the coordinates of the pixels can be moved about with the use of a chaotic map. Pixels are diffused using the SCAN method, while permutations are generated using chaotic maps. Since limitations of wavelet-based approaches include insufficient phase information, inadequate directionality, and sensitivity to shifts.

Another study [35] applied (ICE) Improved Chaos Encryption to strengthen the protection that was based on randomization. The ICE approach was employed to increase the medical encryption's level of security. ICE first partitions the original image into three parts which were: border area, (ROI) Region of interest and (RONI) Region of noninterest. The Lorenz 96 model was applied for medical image encryption. The information would be embedded based on LSB.

In order to guarantee the authenticity of the integrity authentication, ROI has been recovered and returned to its starting position. S-HC-DNA in [36] was an upgraded image encryption scheme to increase the protection afforded to medical images during information-sharing procedures, such as those conducted over the internet. The SHA-3 technique was utilized to compute the hash value of the input image, and the resulting value was utilized as the starting point for the hyper-chaotic system. The input image's intensity value was then transformed into a sequential binary digital stream. In order to improve the encryption performance, the values of the DNA encoding were subjected to algebraic and complementary operations during the hyperchaotic sequence and DNA sequence operation.

The SCAN pattern and tent map are also proposed in [37]. The method consists of a bit plane decomposition, a SCAN-based shuffling process, and a diffusion operation. In order to obtain a more unpredictable result, the SCAN method was implemented on both the upper and lower four-bit planes independently. After that, the XOR operation would be included in the diffusion operation.

Securing E-healthcare image encryption based on a six-dimensional hyperchaotic map (SDHM) was suggested in [38]. This scheme was used to retrieve hidden keys. After that, these keys were applied to the medical images to diffuse them. In general, the proposed SDHM was divided into three sections: the creation of a key, the encrypting procedure, and the decrypting procedure. The key size has been greatly expanded due to the SDHM that was proposed. Thus, the SDHM that has been presented was capable of withstanding various security attacks.

In [39], the author proposed a chaotic-based cryptography architecture for the secure storage and transmission of medical images. The key was first generated by employing the chaotic map approach on the medical image. This produced the initial result. Second, it was implemented in a way that creates confusion both row by row and column by column. In addition, a binary complement operation and a reverse complement operation were used to complete the diffusion process. Images that have been diffused were XORed with key images that have a chaotic appearance. Several attacks were used to evaluate the proposed system's security. According to the simulation results, the created cryptosystem must meet the needs of IoT healthcare applications.

Another study [40] suggested a method for encrypting medical images using chaotic logistic maps and linear feedback shift registers to produce pseudo-random sequences, which were then utilized to form a cipher key by being XORed together. The suggested approach protected several different medical image formats from a wide range of threats.

In [41], the authors presented a novel image encryption algorithm that could be used for both gray and colored medical images. The authors claimed that their algorithm was superior to current encryption methods that were already in use.

The authors in [42] designed a selective image encryption algorithm that was both secure and effective. The encryption method was designed with the foundations of polynomial secret picture sharing and chaotic maps. A polynomial-based secret image sharing (SIS) and a chaotic map system are used to encrypt the essential component of the ROI after image processing techniques are employed to partition the image into a region of interest (ROI) and a region of non-interest (RONI). In order to reduce the amount of time spent encrypting and decrypting data, as well as the amount of computing complexity involved in processing the enormous amount of image data, a preset section of the original image data were encrypted. The experimental results demonstrated the efficiency of Polynomial-

based SIS and chaotic image encryption for the concealment-critical tasks of diffusion and confusion, respectively.

A new, most significant bit (MSB) based reversible data encryption solution for huge amounts of data is proposed in [43]. In the first step, the encrypted domain data undergoes MSB data concealing after the three stages of prediction error detection, fusion error encryption, and substitution data encryption have been taken into account. As a result, the initial phase of the method involves locating and cataloging every instance of incorrect prediction in the source image using a binary map. Then, to fix the mistake in the predictions, a high-capacity reversible data hiding technique (CPHCRDH) is proposed. A map of where mistakes are likely to occur in the prediction process is created, and the original image is preprocessed using this map before encryption takes place. Through MSP prediction, the original, undamaged image can be rebuilt. The simulation experiment on three test cases of CT images of the eyes, body, and brain demonstrates that the suggested method outperforms the selected contrasting methodology across six indicators, including the horizontal and vertical correlation coefficients.

Introducing 2D-LGHM, a brand new Logistic-Gaussian hyperchaotic map in [44]. First, the author builds a 2D Logistic-Gaussian hyperchaotic map (2D-LGHM) with a wide variety of hyperchaos and it finds that it has superior ergodicity and unpredictability based on performance test metrics. In this study, the author develops a novel method for encrypting medical images by using hyperchaotic matrices to randomly disturb pixels and by substituting each pixel's value with those of its neighbors in opposite orientations. An effective application of the chaotic sequence to eliminate neighboring-pixel correlation and universally alter pixel values. The experiment outcomes and performance analysis demonstrate that LG-IES is capable of encrypting a wide variety of medical images into an unrecognizable cipher image that can only be decrypted with the correct secret key.

Table 3 illustrates the state-of-the-art of the various encryption techniques based on chaotic maps.

Table 3. An overview of various encryption techniques based on chaotic maps.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[30]	Introducing double encryption algorithm to preventing hackers from stealing face data.	Chaos and Double Encryption Strategy	Classical images Barbra, Girl, Lena, Reagan	Statistical attacks
[31]	For the purpose of image encoding and decoding	Sine Map, Chaotic Tent Map, and Circulant Matrices	Classical images Lena, Girl, Boat, Baboon, Camera man	Brute-force attacks
[32]	For the purpose of ensuring the reliable transmission of images.	Chaotic image encryption algorithm based on Latin square and random shift	Classical image Lena	-
[33]	Offers the highest possible protection for a select number of devices.	Lightweight Chaotic Cryptosystem	Classical images Lena, Baboon Medical images Chest X-RAY, ECG Signal	-
[34]	In order to ensure the safety of medical images prior to their transmission to the general public via this network.	SCAN and chaotic-map-based image encryption	Medical image baby in womb	-
[35]	Increasing security through randomness.	Lorenz-chaotic encryption with enhancements	Medical image Jaw X-RAY	Various kinds of attacks
[36]	Improvement of medical image safety during data exchanges, particularly online.	DNA coding, the Hash Algorithm 3 (SHA-3), and high-dimensional chaos	Medical image Brain image	Noise and clipping attacks.

Table 3. Cont.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[37]	Accomplishes a high level of safety with minimal effort on the computational front.	SCAN method and chaotic tent map	Different medical images	Statistical and differential attacks
[38]	To ensure the safety of medical images before to their dissemination on public networks.	Six-dimensional hyperchaotic map (SDHM)	Medical images	Security attacks
[39]	For the purpose of assuring the safety of the medical images while they are being sent and stored.	Chaotic security architecture	X-RAY Medical images	Noise Attack
[40]	Avoid unauthorized access to sensitive medical image information.	Chaotic logistic map and linear feedback shift register	Brain MRI chest X-ray	Security attacks like brute-force, man-in-the-middle
[41]	For the purpose of encrypting both black-and-white and color medical photos.	Image blocks and chaos	Different medical images	Differential attacks
[42]	To lower computational costs and save time.	A polynomial-based system for secret image sharing (SIS), as well as a chaotic map system	Brain MRI	Brute force attacks
[43]	Addressing both the limited encrypted data capacity of the technique and the difficulty of recovering encrypted data.	Based on the most significant bit (MSB), a large-capacity reversible data encryption technique	Medical images	Statistical attacks
[44]	To demonstrate exceptional safety and high performance.	Hyperchaotic 2D Logistic-Gaussian Map (2D-LGHM)	Medical images	Security attacks

Measures such as NPCR, UACI, KA, HA, MAE, EI, ET, NA, KS key sensitivity, and PSNR are used to confirm the algorithms' efficacy and strength. The outcomes of the diverse techniques employed in the aforementioned prior investigations are compared in Table 4.

Table 4. The comparison of prior research outcomes.

Ref. No.	Image Details	cc Value	Results						
			NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[30]	Barbra	Hor. −0.000904	99.6036	33.4892	0.995758	7.902155656540	-	-	-
	Girl	Ver. 0.000503	99.6102	33.5023		7.902632365459	-	21.0327	-
	Lena	Diag. 0.001368	99.6059	33.4652		7.902423121654	-	-	-
	Reagan	-	99.6099	33.4899		7.902232165444	-	-	-
	Proposed	-	-	-		-	-	-	-
[31]	Lena	0.0056	-	-	-	7.9990	-	-	-
	Girl	−0.0065	-	-	-	7.9720	-	-	-
	Boat	0.0045	-	-	-	-	-	-	-
	Baboon	0.0016	-	-	-	7.9800	-	-	-
	Camera man	−0.0053	-	-	-	-	-	-	-
Proposed	-	99.6221	33.46	-	-	8736.9	8.7172	-	
[32]	Lena	HOR. 0.0023 VER. 0.0158 DIAG. 0.0147	99.6101	33.4583	-	-	-	-	0.325
[33]	Lena	HOR. −0.00011 VER. 0.0024 DIAG. −0.0012	0.9954	0.2651%	-	7.9762	6.73964×10^3	9.808	-
	Baboon	HOR. 0.0037 VER. −0.0024 DIAG. −0.001	0.9949	0.2389%	-	7.9472	5.5232×10^3	10.7089	-
	Chest X-RAY	HOR. 0.9831 VER. 0.0206 DIAG. −0.00052685	0.9962	0.3442%	-	7.4964	1.1573×10^4	7.4964	-
	ECG Signal	HOR. −0.00022 VER. −0.0566 DIAG. −0.0044	0.9957	0.3533%	-	7.9480	1.1970×10^4	7.3498	-
	[34]	baby in womb	-	99.85	-	-	-	-	-
[35]	Jaw X-RAY	-	99.62	33.41	-	7.9974	-	104.07	-
[36]	Brain 1	0.00014	53.3930	19.9316	-	7.6554	-	-	-
	Brain 2	0.00049	50.2161	19.3573	-	7.6684	-	-	-
[37]	Medical image 1	-	99.6658	43.9856	-	7.9965	33.8168	22.8395	-
	Medical image 2	-	99.6445	41.3774	-	7.9972	30.7966	23.2458	-
	Medical image 3	-	99.6292	42.0747	-	7.9970	57.8667	20.5065	-
	Medical image 4	-	99.6307	40.4066	-	7.9974	64.2554	30.0517	-
	Medical image 5	-	99.6445	43.0771	-	7.9969	26.9480	24.8255	-

Table 4. Cont.

Ref. No.	Image Details	Results							
		cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[38]	CTA	HOR. 0.0076	-	-	-	7.59	-	59.41	-
		VER. 0.0052							
		DIAG. 0.0049							
	BMRI	HOR. 0.0051	-	-	-	7.53	-	58.14	-
		VER. 0.0059							
		DIAG. 0.0045							
	DM	HOR. 0.0021	-	-	-	7.38	-	60.22	-
		VER. 0.0072							
		DIAG. 0.0015							
	FS	HOR. 0.0065	-	-	-	7.43	-	60.52	-
		VER. 0.0037							
		DIAG. 0.0032							
	US	HOR. 0.0006	-	-	-	7.39	-	58.65	-
		VER. 0.0027							
		DIAG. 0.0062							
[39]	Crop attack 0.5%	0.9962	-	-	-	-	39.51	32.16	-
	Crop attack 1.0%	0.9900	-	-	-	-	104.96	27.92	-
	Crop attack 2%	0.9661	-	-	-	-	357	22.60	-
	Salt & pepper noise 0.001	0.9994	-	-	-	-	6.40	40.06	-
	Salt & pepper noise 0.01	0.9893	-	-	-	-	112.54	27.61	-
[40]	-	-	-	-	-	-	-	-	-
[41]	Image 1	HOR. -0.0093 VER. 0.0025 DIAG. -0.0024	99.6010	33.4389	-	7.9993	-	5.1192	-
[42]	Brain MRI	HOR. -0.0016 VER. 0.0028 DIAG. 0.0006	99.62	33.57	-	7.9992	-	-	0.5331
[43]	Medical image	-	-	-	-	-	-	-	-
[44]	Proposed	HOR. -0.0027 VER. 0.0031 DIAG. 0.0011	99.6009	33.4596	-	7.9998	-	-	-

The optimal value of UACI is 34. However, in some papers appears % as a statistical analysis of a group of images.

6.2. Encryption Based on Elliptic Curve Cryptography (ECC)

The characteristics of algebraic curves serve as the foundation for the construction of elliptic curves. The use of an elliptic curve was integral to the creation of a public key encryption method by Koblitz and Miller. Elliptic curve encryption's main advantages are its low key size and high processing efficiency [45]. The function of an elliptic curve within an image encryption is illustrated in Figure 7 [29].

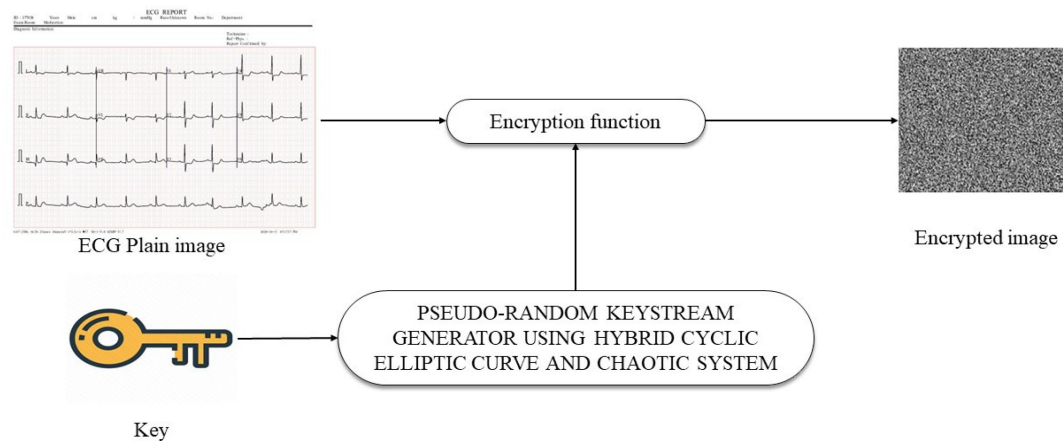


Figure 7. The encryption of images using ECC [29].

In [46], an existing encryption system that was created with elliptic curve cryptography (ECC) and a Hill cipher was analyzed through the process of cryptanalysis. Affine Hill ciphers were utilized to spread the original image matrix into 4×4 blocks, which were then employed as keys in the scheme. Most importantly, the selected elliptic curve was used to construct the chaotic map's primary parameters. Bit-wise XOR was then performed with the produced Arnold map sequence on top of the scrambled data. According to the results of the research, the current system was insecure and could be broken by a brute-force attack.

ECC also proposed in [47] as a security for medical images in the IoT which was proposed by combining visual cryptography and Optimal Elliptic Curve Cryptography (IoT). Using an imperialist competitive algorithm, the best possible key was constructed. The ESEA strategy that has been presented shortens the amount of time needed to upload files and cuts down on the amount of memory that was consumed by encryption. The simulation results showed that the suggested system had a good chance of achieving the optimal global solutions faster and more precisely than the current methods.

In [48], the authors discussed a new cryptographic approach for protecting medical images created by IoHT healthcare devices by applying an advanced optimization technique, based on elliptical curves and Grasshopper Particle Swarm Optimization (GOPSO) to choose the best possible key to protect medical images. Compared to previous optimal encryption methods, the study's findings showed that the proposed algorithm was secure and resistant against a wide range of assaults. The results of the experiments demonstrate increased sensitivity of the keys, improved accuracy of the encryption, and excellent resistance to statistical attacks.

In this study [49], the authors discuss a novel cryptographic method for securing medical images that rely on Hill cipher in conjunction with ECC (ECCHC). The authors employ this strategy to overcome the vulnerability of certain encryption techniques to specific attacks and the difficulty of using a key length that is resistant to brute-force methods of decryption. The ECCHC scheme was found to be secure and perform better than competing schemes through extensive testing and research.

A homomorphic encryption method based on an elliptic curve was presented in [50] for use with medical images. The author used the improved ECC to bring about the

addition homomorphism and the multiplication homomorphism. It has recently been demonstrated that cryptosystems based on ECs over finite rings may offer higher security than those based on other algorithms, such as the factorization problem or the discrete logarithm problem.

Prompted by this realization, a fresh approach to cryptography based on ECs over finite rings was introduced in [51]. The approach consists of three primary phases, the first of which involves masking the simple image with points of an EC across a finite ring. Step two involved generating diffusion within the masked image by transferring the EC through the finite ring to the EC over the finite field. In order to produce a large amount of confusion in the plain text, the author first constructed a substitution box (S-box) based on the ordered EC. This box was then used to permute the pixels of the diffused image to produce a cipher image.

Upgraded image encryption using MAES-ECC was developed for use in embedded systems in [52]. This technique employed a modified variant of AES in which the mix column transformation phase was replaced with a permutation-based shift of columns, resulting in reduced temporal complexity while maintaining the Shannon principle of diffusion and confusion.

Using the elliptic curve cryptosystem and the hill cipher, the author of [53] created a robust image encryption technique. Hill Cipher transforms a symmetric encryption method into an asymmetric one, making it more secure and resistant to attacks. In this technique, the burden of locating and disseminating the inverse key for decryption was eliminated by using a self-invertible key matrix for the purpose of encrypting and decrypting confidential information. Intruders would have a difficult time deciphering this strategy because the key matrix that used was based on ECC. The results of the simulation have shown that the method was effective in both protecting against a variety of attacks and saving time.

The author in [54] used a moving S-box and a random additive mask to encrypt images. The approach used two methods: the first was the use of random nonce and safe hash algorithm in computing per-image Henon map setup, and the second was the use of elliptic curve encryption in securing the secret key. The suggested approach achieved encryption speeds that were close to 60 MB/s due to its excellent computational efficiency.

In [55], the study sought to accomplish two goals at once. First, by establishing a total order on an EC over a prime field, the author introduced new techniques for building s-boxes and generating pseudo random numbers (PRN). The second component was a two-phase image encryption system that was based on the recently established s-box and PRN generating method. The plain-image would be first confused by a suggested PRN, which was then masked by a fully dynamic S-box in this security system. This process began by diffusing the plain-image. The proposed methods were capable of constructing cryptographically robust S-boxes and PRNs with high entropy and excellent resistance to contemporary image cryptanalysis. Table 5 illustrates the state-of-the-art of the various encryption techniques based on Elliptic Curve Cryptography (ECC).

Table 5. An overview of various encryption techniques based on ECC.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[46]	In order to send multimedia files quickly and securely	Hill cipher, Elliptic Curve Cryptography, and a 3D Chaotic Map	Classical images Jet, House, Barbra, Baboon, Pepper, Lady	brute force attacks
[47]	suggested for the security of medical images transmitted over the Internet of Things	Incorporating Optimal Elliptic Curve Cryptography with visual cryptography	Different medical images	-

Table 5. Cont.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[48]	in order to preserve sensitive patient data and ensure the privacy of their medical records	to improve IoHT, a hybrid approach based on a cryptographic method (ECC with GOPSO)	Different medical images	statistical attacks
[49]	in order to solve the problem regarding the level of security provided by an image encryption method	use a combination of the Elliptic Curve Cryptosystem and the Hill Cipher (ECCHC)	Classical image Lena & Medical image DICOM	various knowing attacks
[50]	To enhance the security of elliptic curve algorithm and implemented during the process of encrypting medical images	combining homomorphic encryption and elliptic curve cryptography	Medical images	initial value & anti-attack ability.
[51]	To offers a great level of security with a small key size	ECs over finite rings	Classical images Lena, Barbara	linear, differential, and statistical attacks
[52]	In order to present a method that encrypts images of a huge size while maintaining a high level of security in a timely manner	ECC (Elliptic curve), MAES (Modified AES)	Classical images Lena, Peppers, Baboon Medical image 3D scanner ankle	Statistical attacks, Noise attack, Differential attacks and Brute force attack
[53]	Create a system with enhanced security that can withstand a variety of attacks	Hill cipher, Arnold cat map, Hyper Chaotic Lorenz Generator (HCLG), and ECC	Classical image Lena Medical image DICOM	Data loss attacks, noise attacks, Differential-statistical attacks, occlusion attacks, and exhaustive search attacks
[54]	in order to strengthen defenses against assaults	S-boxes derived from the Henon map and elliptic curve	Classical images Cameraman Lifting body	chosen-plaintext and chosen-ciphertext attacks
[55]	maintaining the same key size while increasing security	S-Box and the generation of pseudo-random numbers (PRN) with ECC	Classical images Circuit, Boat, Lena, Pepper (Black & White)	linear attacks

The outcomes of the diverse techniques employed in the aforementioned prior investigations are compared in Table 6.

Table 6. The comparison of prior research outcomes.

Ref. No.	Image Details	Results							
		cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[46]	Jet	HOR. 0.0002	99.6102	33.4049	-	7.9978	R 4.192 × 10 ⁴	R 8.145	-
		VER. −0.0024					G 7.180 × 10 ⁴	G 7.547	
		DIAG. 0.0026					B 8.993 × 10 ³	B 7.128	
	House	HOR. −0.0019	99.6294	33.3503	-	7.9978	R 9.941 × 10 ³	R 8.254	-
		VER. 0.0001					G 6.120 × 10 ⁴	G 8.548	
		DIAG. 0.0029					B 8.973 × 10 ³	B 8.489	
	Barbara	HOR. 0.0017	99.6345	33.3456	-	7.9979	R 1.257 × 10 ⁴	R 8.189	-
		VER. −0.0020					G 9.180 × 10 ³	G 9.512	
		DIAG. 0.0047					B 7.257 × 10 ⁴	B 8.178	
	Baboon	HOR. 0.0021	99.6236	33.3130	-	7.9978	R 9.256 × 10 ³	R 6.235	-
		VER. 0.0011					G 8.595 × 10 ³	G 7.249	
		DIAG. 0.0011					B 8.980 × 10 ⁴	B 6.954	
	Pepper	HOR. 0.0004	99.6398	33.3188	-	7.9976	R 8.120 × 10 ⁴	R 9.517	-
		VER. 0.0019					G 1.235 × 10 ⁴	G 8.865	
		DIAG. 0.0003					B 4.985 × 10 ³	B 8.562	
	Lady	HOR. 0.0023	99.5896	33.4449	-	7.9976	R 9.456 × 10 ³	R 7.214	-
		VER. 0.0041					G 8.156 × 10 ³	G 9.121	
		DIAG. 0.0014					B 9.562 × 10 ³	B 8.128	
[47]	Medical image 1	0.99	-	-	-	-	0.08	61	1341
	Medical image 2	0.98	-	-	-	-	0.09	59	1068
	Medical image 3	0.99	-	-	-	-	0.11	61	956
	Medical image 4	0.97	-	-	-	-	0.07	61	3241
	Medical image 5	0.99	-	-	-	-	0.12	62	4253
	Medical image 6	0.99	-	-	-	-	0.08	61	6254
	Medical image 7	0.98	-	-	-	-	0.11	61	3247
[48]	Medical image 1	-	-	-	-	-	0.10	51.21	-
	Medical image 2	-	-	-	-	-	0.12	49.23	-
	Medical image 3	-	-	-	-	-	0.15	58.33	-

Table 6. Cont.

Results									
Ref. No.	Image Details	cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[49]	Lena	HOR. 0.016727 VER. 0.156755 DIAG. 0.009032	-	30.3842	-	7.9970	-	8.5950	1.442 _(Km = 4 × 4) 1.82 _(Km = 8 × 8)
	DICOM	HOR. 0.599602 VER. 0.605063 DIAG. 0.449645	80.2094	17.0887	-	3.399602	-	4.753544	2 _(Km = 4 × 4) 2.3 _(Km = 8 × 8)
[50]	Medical image 1	HOR. 0.0015 VER. 0.0008 DIAG. 0.0021	99.23	39.58	-	0.796	-	-	-
	Medical image 2	HOR. 0.0041 VER. 0.0022 DIAG. 0.0018	99.18	38.59	-	0.797	-	-	-
[51]	Lena	HOR. −0.0006 VER. −0.0000 DIAG. −0.0005	99.64	33.44	-	7.9994	-	-	-
	Barbara	HOR. 0.0007 VER. 0.0014 DIAG. −0.0005	-	-	-	7.9993	-	-	-
[52]	Lena	HOR. −0.00591 VER. −0.00145 DIAG. −0.01029	99.6773	33.4769	-	7.9998633	-	-	0.2731
	Scanner Ankle	HOR. −0.0037 VER. −0.0320 DIAG −0.01093	99.8370	33.74291	-	7.99999	-	-	0.2731
[53]	Lena	HOR. 0.00016384 VER. 0.00082884 DIAG. 0.0020	-	30.3842	-	7.99933	-	8.5950	1.442s
	DICOM	HOR. 0.002180 VER. 0.003391 DIAG. 0.000272	99.9950	34.1222	-	7.997844	-	4.790935	2s

Table 6. Cont.

Results									
Ref. No.	Image Details	cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[54]	Cameraman	HOR. −0.0039 VER. 0.0003 DIAG. 0.0047	99.6086	33.4409	-	7.9973	-	-	-
	Liftingbody	HOR. 0.0015 VER. 0.0052 DIAG. −0.0028	99.6087	33.4308	-	7.9994	-	-	-
[55]	Circuit	HOR. −0.0007 VER. −0.00005 DIAG. 0.003	99.5796	33.6686	-	7.9796	-	-	-
	Boat	HOR. 0.0005 VER. −0.0011 DIAG. 0.0009	99.5956	33.2872	-	7.9973	-	-	-
	Lena	HOR. 0.0012 VER. 0.0003 DIAG. 0.0010	99.5964	33.4762	-	7.9993	-	-	-
	Pepper	HOR. 0.0012 VER. −0.0015 DIAG. −0.0017	99.6117	33.5106	-	7.9994	-	-	-

6.3. Encryption Based on DNA (Deoxyribonucleic Acid)

Deoxyribonucleic acid (DNA) technology has recently touched many fields, including the medical system, information science, etc. Information was stored in DNA molecules, which carry genetic code that could be converted from one form to another. Pseudo-DNA technology was a simulation environment for DNA-based biological experiments recently developed by scientists. DNA encryption has been advanced by this idea [56].

The DNA-based image encryption mechanism is depicted in the block diagram found in Figure 8 [29]. The first step was to separate the image into its individual color channels: red (R), green (G), and blue (B). Each of these three channels was converted into a binary matrix. These matrices were subsequently encoded according to the rules of DNA encoding. DNA operations were performed on the encoded matrices, which scrambled the similarity between pixel values. Applying the decoding rules results in a new set of binary matrices. Eventually, a cipher-colored image was created by combining these three color channels [57].

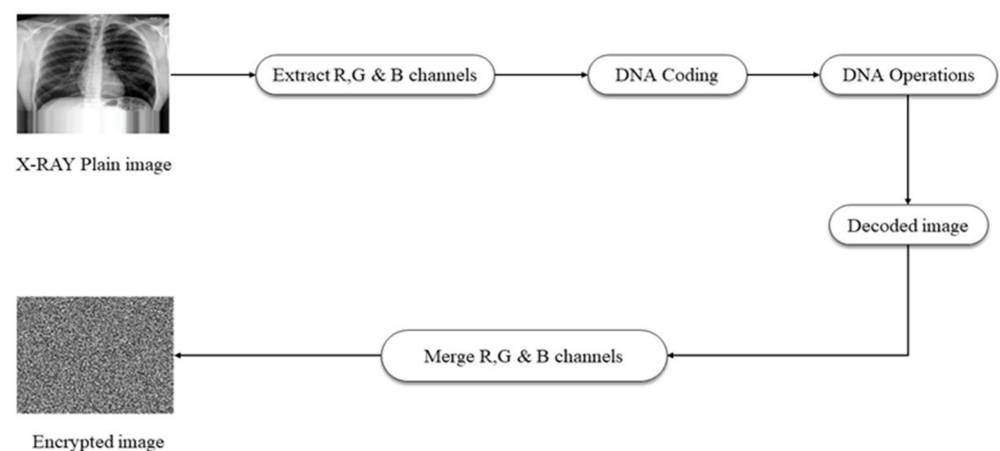


Figure 8. The encryption of images using DNA [29].

In [58], a method for encrypting images using DNA coding and annealing was presented as a possible solution. The image pixels were modified with the chaotic system's pseudo-random number sequence by adding the mutation step to the conventional scrambling and diffusion framework. This outcome was in an image that was more difficult to decipher. There was an 80% probability that every pixel would have just one bit reversed and a 20% chance that every bit would be reversed. Authors generated ciphertext images by applying the same encryption approach to the RGB, YC, and BG channels of a color image.

To secure sensitive medical images, a new cryptosystem is presented in [59]. Using DNA sequencing, Knight's trip map, intertwining chaotic maps, and affinity transforming. First, a B1 pixel DNA-coded matrix is created from the original medical image. The remaining pixels in matrix B2 were deployed on the pixel index values selection using DNA coding. After that, the system and control parameters generated chaotic sequences, which were depicted as a through-like pattern in the chaotic map. The performance analysis results showed that the suggested DMIES effectively reduces the risk of attacks like differential cropping, exhaustive probing, noise, and statistical analysis.

In [60], The image was encrypted using three different stages: one phase of confusion and two phases of diffusion. In the first stage of diffusion, DNA XOR was used to partially encrypt the image by operating on DNA-encoded image pixels and a hyperchaotic sequence. The next step involved using a Baker map to scramble the placements of each pixel in the partially encrypted image. A two-dimensional discrete cosine transform (DCT) was applied to the image in the diffusion phase, which converted the information from the spatial domain to the frequency domain. Due to its key sensitivity and resistance to various crypt-analytic attacks, the proposed algorithm demonstrated a high level of security.

For medical image encryption, Ref. [61] suggested system combines the hyperchaotic RKF-45 random sequence with DNA computation. The suggested framework used the RKF45 approach to generate chaotic sequences. After that, a 4-dimensional hyperchaotic integration was used to produce a random key sequence. The proposed framework cipher's unpredictability and efficiency were also improved by adopting DNA addition and subtraction operations. According to the findings, the suggested HC-RK45-DNA framework could withstand differential attacks.

A new DNA-based medical image encryption method and a 3D unified chaotic system were presented in [62] to increase the safety of medical image storage. In the beginning, a key value was constructed by using the input image for the sake of avoiding specific plaintext attacks. The execution of the chaotic system and its starting values were determined by this freshly produced key value. Here, a chaotic system was driven to generate a pseudorandom sequence that could be used for image scrambling and diffusion, as well as for converting pixels to DNA bases. The DNA bases were then converted and decoded using straightforward reversible methods. First, random numbers were used to swap out DNA bases, and then the bases were decoded to produce a new pixel value.

An image steganography scheme based on DNA was proposed in [63]; the proposed method involved encrypting the image to be concealed by using a DNA tape as a key, which was agreed upon by both parties, executing the hybridization process, and performing the hiding process in a different way, also dependent on the same key. In addition, the proposed method included performing the hybridization process. Implementing the BIO-XOR procedure between the DNA strand created in the previous stage and another DNA strand follows the hybridization process for the sequence of nitrogenous bases. The author in [61] presented a keyless process that helps to increase the unpredictability of the original image. The suggested approach used a generalized version of Arnold's Cat Map to add to the chaos. Additionally, a new diffusion mechanism has been implemented, and it worked on two different levels: the pixel level and the DNA plane. It included all potential DNA encoding, decoding, and XOR rules, chosen in a random-ish fashion according to the values of a chaotic 2D-Logistic Sine Coupling Map. This strengthened the cipher image against brute force and statistical attacks, and it became complicated for an intruder to decipher the cipher and see the original image without the correct key.

The proposed algorithm for medical image encryption in [64] used 2D-LSCM. In the formulated cryptosystem, 2D-LSCM performed the primary confusion-diffusion. The algorithm suggested a new masking strategy, which was one that did not require a key. In order to increase the entropy of the image, this step was performed before the confusion and diffusion process. The number of iterations in the ACM-based confusion stage has been optimized to produce a heavily garbled image while avoiding periodicity. The most crucial part of this cryptosystem was the diffusion algorithm, which modified the image's pixel values at both the bit and pixel levels.

Hyper chaos and DNA encoding were introduced in [65]. It consisted of four stages, which were the formation of starting values of a chaotic system, the generation of key streams, scrambling, and diffusing. The suggested approach provided the following benefits. The first step was to extract ROI images and encrypt select crucial pixels. It could decrease the total amount of encryption pixels, which would assist in reducing the encryption time. Second, in order to lower the pixel correlation, hyperchaotic sequences were implemented. Lastly, because of the utilization of DNA encoding, it was possible to save resources that were used for computational storage.

A selective digitalization of medical images utilizing dual hyper chaos maps and DNA sequencing were proposed as methods of image encryption in [66]. First, a DNA-encoded matrix C1 was created from the selected pixels in the original medical digital image by applying all DNA rules depending on the pixel index value, and a DNA-encoded matrix C2 was created from the remaining pixels. The parameters and system elements of the dual hyperchaotic map were used to generate the chaotic sequences. Selected pixels of the DNA-encoded matrix, C1, were scrambled using the dual hyperchaotic map. The DNA

XOR method was used to combine the DNA-encoded matrix C1 that has been scrambled with the DNA-encoded matrix C2. After applying all of the DNA decoding rules to the combined DNA-encoded matrix, the resulting binary image was transformed to grayscale to produce the cipher image.

The authors in [67] proposed a DNA masking combined with the Secure Hash Algorithm (SHA-2) in a hybrid model. With the purpose of making the diffusion process more effective, a hybrid chaotic function was applied. DNA XOR was used in the confusion step. In order to produce one-time keys from plain images and secret hash keys, the Secure Hash Algorithm 2 (SHA-2) was employed. The encryption key was this hash value. The pixels were shuffled using random sequences as part of the diffusion process. Random sequences were produced using the chaotic hybrid map. These sequences were utilized to randomize the image. In order to confuse things, authors used DNA XOR to scramble the original image's pixel values.

The suggested system in [68] consisted of a transmitter and a receiver that were responsible for performing the tasks of encrypting and decrypting, respectively. Despite their different functions, both components had the same structure design with two effective modules, which were: A Content-Aware Permutation and Diffusion Module and a Random-DNA-Encoding Module. The former constructed a random encryption rule selector in the DNA encoding process, which boosted security by constructing an abundance of random mappings from image pixels to calculations and significantly increased key sensitivity. The second part of the program created a permutation sequence that did more than save the values of individual pixels—it also disrupted the strong association between neighboring pixels within the same patch. Table 7 illustrates the state-of-the-art encryption techniques based on Deoxyribonucleic Acid (DNA).

Table 7. An overview of various encryption techniques based on DNA.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[58]	To overcome the huge capacity of image data and the disparity among pixels, resulting in restricted randomization.	The encoding of DNA and the annealing process	Classical image Lena, Plain, Cameraman, Baboon, Peppers	Cropping and differential attacks
[59]	Seeks to develop a system for the encryption of medical photographs.	DNA sequencing, the Knight's travel map, the intertwined chaotic maps, and affinity transformation	Medical images CT-image, Ultrasound-image, MRI-image, X-ray-image, ECG-image, Lena image	Statistical, differential, exhaustive, cropping, and noise attack
[60]	In order to enhance the quality of encryption by using a system that is DNA encoded.	By using the DNA XOR algorithm, a modified version of the Vigenère cipher, the Diffie- Hellman key exchange, the Arnold map, and the Baker map, as well as	Classical image Lena, Baboon	Brute force attack
[61]	Improving the security of medical image transformation and patient data confidentiality by developing and implementing a strong medical encryption framework.	Hyperchaotic RKF-45 random sequence method and DNA computing	Medical images	Differential attacks

Table 7. Cont.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[62]	Creating an efficient method that can encrypt images, with a focus on medical images due to their unique properties.	Dynamic DNA coding and the 3D Unified Chaos System.	Medical images	Distinct types of cryptographic attacks
[63]	Presenting a new approach of steganography that takes advantage of DNA's characteristics.	DNA Properties	Classical images	-
[64]	Present a secure technique for encrypting medical photos.	The use of bit-level diffusion with DNA coding	Medical and natural images	Differential, occlusion, and noise attacks
[65]	Reduce the total number of encryption pixels to make the encryption process faster while maintaining the same level of security.	Fast and robust Deoxyribonucleic acid encoding and fuzzy C-means clustering image segmentation technique	Medical images	Noise attacks, clipping attacks, statistical analysis, and so on
[66]	In order to ensure the safety of a digital medical image.	DNA cryptography and dual hyperchaotic map	Medical images	Different types of attacks
[67]	Enhance the security of the cryptosystem.	DNA masking combined with the Secure Hash Algorithm (SHA-2) in a hybrid model	Medical images	Statistical and exhaustive attacks
[68]	In order to guarantee the confidentiality of cipher images.	Module for Content-Aware Permutation and Diffusion, and Module for Random-DNA Encoding	Medical images	Various attacks

The outcomes of the diverse techniques employed in the aforementioned prior investigations are compared in Table 8.

Table 8. The comparison of prior research outcomes.

Ref. No.	Image Details	Results							
		cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[58]	Lena	HOR. −0.0002 VER. −0.0011 DIAG. 0.0015	99.5956	33.4762	-	7.9995	-	-	-
	Plain	HOR. −0.0028 VER. 0.0002 DIAG. −0.0016	99.6212	33.4229	-	7.9995	-	-	-
	Cameraman	HOR. −0.0027 VER. −0.0013 DIAG. −0.007	99.6231	33.4556	-	7.9995	-	-	-
	Peppers	HOR. 0.0014 VER. 0.0012 DIAG. 0.0011	99.6056	33.4904	-	7.9995	-	-	-
	Baboon	HOR. 0.0029 VER. 0.0014 DIAG. −0.0006	99.6220	33.4436	-	7.9995	-	-	-
[59]	Lena	-	99.643	33.574	-	7.9976	9130.17	8.56	-
	CT-image	-	99.789	33.487	-	7.9975	15,145.68	6.36	-
	Ultrasound-image	-	99.781	33.483	-	7.9994	12,820.64	7.09	-
	MRI-image	-	99.843	33.598	-	7.9977	16,814.41	5.91	-
	X-ray-image	-	99.809	33.423	-	7.9996	12,077.12	7.35	-
ECCG-image	-	99.668	33.447	-	7.9971	11,671.33	7.49	-	
[60]	Lena	HOR. 0.0005 VER. 0.0032 DIAG. 0.0034	99.5585	33.2983	-	7.9975	-	9.9211	0.5623
	Baboon	HOR. 0.0002 VER. −0.0041 DIAG. 0.0035	99.5952	34.0913	-	7.9991	-	8.5361	0.5623

Table 8. Cont.

Results									
Ref. No.	Image Details	cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[61]	IMG01	HOR. −0.00087 VER. 0.00021 DIAG. −0.00021	99.105679	32.762518	-	7.99649256554477	-	-	-
	IMG02	HOR. −0.00082 VER. −0.00109 DIAG. 0.00089	99.565625	33.327747	-	7.98910516850633	-	-	-
	IMG03	HOR. −0.00163 VER. 0.00048 DIAG. −0.00051	99.603908	33.014542	-	7.99873639562868	-	-	-
	IMG04	HOR. 0.00037 VER. 0.00015 DIAG. 0.00014	99.603908	33.012166	-	7.9989390680445	-	-	-
[62]	Sample 1	HOR. 0.0068 VER. −0.0136 DIAG. 0.0045	99.603	33.4062	-	7.9943	-	-	-
	Sample 2	HOR. −0.0152 VER. 0.0054 DIAG. −0.0058	99.5987	33.3974	-	7.9954	-	-	-
	Sample 3	HOR. 0.0035 VER. 0.0054 DIAG. −0.0067	99.6035	33.4051	-	7.9911	-	-	-
[63]	Encrypted image1	−0.0059	-	-	-	-	1.5000×10^4	6.3698	-
	Encrypted image2	0.0153	-	-	-	-	1.0539×10^4	7.9028	-
	Encrypted image3	-9.6203×10^{-4}	-	-	-	-	9.2446×10^3	8.4719	-

Table 8. Cont.

Results									
Ref. No.	Image Details	cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[64]	CT-scan	HOR. −0.0016 VER. 0.0012 DIAG. 0.0200	99.5544	0.3331%	-	-	-	-	-
	MRI	HOR. 0.0125 VER. −0.0079 DIAG. −0.0077	99.5316	0.3348%	-	7.9967	-	-	-
	Ultrasound	HOR. 0.0125 VER. 0.0040 DIAG. −0.0066	99.5789	0.3344%	-	-	-	-	-
	X-ray	HOR. 0.0019 VER. −0.0096 DIAG. −0.0136	99.5956	0.3351%	-	-	-	-	-
	Boat	HOR. −0.0119 VER. 0.0047 DIAG. 0.0066	99.5998	0.3355%	-	7.998973	-	-	-
	Baboon	HOR. 0.0172 VER. −0.0064 DIAG. −0.0042	99.6136	0.3352%	-	7.998621	-	-	-
	[65]	sample_1	HOR. 0.0241 VER. −0.0365 DIAG. 0.0345	99.6424	33.8123	-	7.99167	-	25.85807
sample_2		HOR. 0.0154 VER. −0.0311 DIAG. −0.0207	99.5892	33.1487	-	7.98883	-	37.07617	2.36
sample_3		HOR. 0.0045 VER. 0.0438 DIAG. 0.0337	99.5489	33.1348	-	7.99060	-	-	2.36
sample_4		HOR. −0.0054 VER. −0.0212 DIAG. −0.0797	99.6647	33.4478	-	7.98813	-	-	2.36

Table 8. Cont.

Results									
Ref. No.	Image Details	cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[66]	CT image	HOR. 0.996 VER. 0.999 DIAG. 0.997	99.7	33.7		7.86	730.1	5.8	0.24
	MRI image	HOR. 0.995 VER. 0.992 DIAG. 0.996	99.7	33.55		7.85	767.07	5.9	0.24
	Ultrasound image	HOR. 0.994 VER. 0.992 DIAG. 0.992	99.6	33.57		7.83	710.07	5.9	0.25
	X-ray image	HOR. 0.995 VER. 0.995 DIAG. 0.996	99.8	33.29		7.89	780.12	5.7	0.2
	ECG image	HOR. 0.993 VER. 0.996 DIAG. 0.991	99.6	33.63		7.8	708.3	5.3	0.25
[67]	Average	HOR. 0.9439 VER. 0.9402 DIAG. 0.8908	99.600124	33.459415	-	7.997862	-	-	-
[68]	X-ray1	VER. 0.0021 HOR. 0.0029 DIAG. 0.0016	-	-	-	-	-	-	-
	X-ray2	VER. -0.0012 HOR. 0.0023 DIAG. -0.0009	-	-	-	-	-	-	-
	COVID-CT1	VER. -0.0008 HOR. 0.0012 DIAG. -0.0019	-	-	-	-	-	-	-
	COVID-CT2	VER. 0.0009 HOR. 0.0015 DIAG. 0.0023	-	-	-	-	-	-	-
	MRI	VER. -0.0018 HOR. -0.0022 DIAG. 0.0014	-	-	-	-	-	-	-
	Proposed	HOR. 0.0014 VER. 0.0009 DIAG. 0.0004	99.6841	33.5539	-	7.9992	-	-	-

6.4. Encryption Based on PQC (Post Quantum Cryptography)

This means algorithms for cryptography that are guaranteed to be secure even when attacked by quantum computers. As a result of their superior speed in performing specific mathematical operations compared to conventional computers, quantum computers pose a threat to several of the currently-used cryptographic techniques, such as RSA and elliptic curve cryptography (ECC). Traditional cryptographic methods that rely on the hardness of mathematical problems, such as integer factorization or discrete logarithms, are vulnerable to quantum computers, despite the former's impressive computational capacity for particular issues. Shor's algorithm [69] is just one example of a quantum algorithm that can efficiently address these challenges, which undermines the credibility of many currently used cryptographic systems. Post-quantum cryptography can be accomplished using a variety of methods, including the following:

1. Lattice-based cryptography: Many methods used in post-quantum cryptography can be reduced to solving lattice problems. Certain difficulties in addressing issues on high-dimensional lattices are the basis for these algorithms. Regev proposed the first standard LWE-based lattice-based encryption technique in [70]. Using quantum processing, this approach factors huge integers by equating their prime number phases expressed as sine waves. This is an important step toward addressing the discrete logarithm issue, which is the focus of many modern cryptographic algorithms [71].
2. Code-based cryptography: In order to generate secure cryptographic protocols, code-based cryptography makes use of error-correcting codes. These methods are built on the fact that deciphering random linear codes is extremely difficult. Two relatively straightforward Code-based cryptographic methods bear Robert McEliece's name and Harald Niederreiter [72].
3. Multivariate cryptography: Cryptographic schemes in multivariate cryptography are founded on systems of multivariate polynomial equations. These schemes are secure because of the difficulty in solving systems of polynomial equations.

A new method for hiding information in medical images employing quantum walking, 3-dimensional chaotic systems, and a modified PSO algorithm is introduced in [73]. The method proposed here involves incorporating a private medical photograph into a publicly-available cover photo. The customized PSO algorithm is run using a 3-D chaotic system and quantum walks, and the generated velocity sequence is used to replace the secret data, while the position sequence is used to choose which location in the carrier image will be used to host the substituted confidential data. This form of image steganography can be applied to both black-and-white and colored photos. A PSNR of 44.1 is achieved on average with the introduced technique, and its embedding capacity is 2 bits per byte.

Quantum selective encryption is being studied as a potential new way of protecting sensitive medical images in [74]. By performing operations on the bit-planes of the images in accordance with a key, the suggested approach successfully encrypts ROI (also known as a region of interest). For a BRQI (Bitplane Representation of Quantum Image) with $2n$ pixels and a key length of m , we have estimated the time complexity of the introduction approach, which offers a huge improvement over its traditional equivalent. In contrast to the time constraints, the size of medical images has no bearing on the method.

In order to ensure the safety of quantum-encrypted medical images, the authors of [75] presented a novel framework. Before being encrypted using the suggested method and sent to the cloud, patient photos are first converted to a NEQR (Novel Enhanced Quantum Representation) representation at a central site. The suggested technique employs a three-step encryption process for its various stages of operation. Quantum-controlled picture preparation, Select secret map keys, and Quantum picture encryption using a scrambled state.

Encryption and decryption of medical images using symmetric cryptography with a chaotic map and a key generator (KG) based on quantum mechanics presented in [76]. The three main phases of the technique are, first, the production of random cipher codes; second, the training of an encryptor and a decryptor based on gray relational analysis

(GRA); and finally, the assessment of the encrypted image. To generate cipher codes for substituting values of pixels (substitution technique) in a 2D image using 256 key-space cipher codes, the chaotic map is combined with a quantum-based key generator (KG) to boost the chaotic complexity and unexpected levels.

The GRA models 1 and 2 are used to train the cipher codes for an encryptor and a decryptor, respectively. A method for quantum watermarking of images is proposed in [77]. Arnold's cat map is used in this approach to introduce chaos into the enlarged watermark. The presented technique relies on the encrypted secret image and the controlled-"NOT" image, both of which are derived from the logistic map. The embedding procedure generates a key matrix that plays a crucial role in improving visual quality but is also utilized to bolster security. In the process of extraction, in addition to the key matrix, control parameters are necessary in order to operate the logistic map.

An original quantum LSB For quantum images of color, a steganographic technique based on the Gray code, has been developed by the authors in [78]. The described data concealing technique makes use of the gray code to conceal a $2m \times 2m$ grayscale image within a $2n \times 2n$ colored image (the "secret image" and "cover image," respectively). In advance of the embedding process, a quantum Hilbert image scrambling technique was used to encrypt the hidden image. Since the key is short, it can be quickly and readily transmitted across the quantum transitional channel from sender to recipient.

Also, A strong protocol for quantum watermarking that employs both the least significant and most significant bits is proposed in [79]. Extraction of the watermarked image using the present protocol is more secure since it requires the production of two key images (scrambling key). Using a novel scrambling technique, the grayscale watermark image is transformed into a scrambled binary image that guarantees the original watermark image cannot be recovered by any attacker, even if the attacker recovers the scrambled binary image. The results of the simulation that were given reveal a superior peak-signal-to-noise ratio, which demonstrates that the cover image undergoes fewer changes while the method is being performed.

Ref. [80] proposed a strategy for quantum steganography that makes use of the two LSBs to conceal a picture with dimensions of $2n_1 \times 2n_1$ within one of dimensions $2n \times 2n$. The proposed technique has good visibility and high capacity, and it does not require the original cover image or original secret image for the extraction process.

The author has shown the first working version of the Ed448 DSA protocol in [81], which is designed to run on the ARM-based Cortex-M4 processor found in many low-end devices. The evaluation findings of the performance are based on the implementation design using only C code and the assembly language for the specific target being evaluated. Finally, the achieved performance describes that the design is resistant to fault and side-channel attacks.

The first implementation of HPKE is immune to the problems that quantum computers pose for asymmetric algorithms introduced in [82]. Using two different postquantum key encapsulation strategies and a wide range of plaintext sizes, we evaluate the efficacy of PQ-only and PQ-hybrid HPKE variants. The system has been expanded to enable both PQ-only and PQ-hybrid choices, and it has been merged with two PQ KEM algorithms that were developed during Round 3 of the PQ Project by NIST.

Ref. [83] provides a study of the energy needed to run potential PQC algorithms using data collected from extensive testing on a Cortex M4-based reference platform. The data transmission costs of PQC algorithms, which are predicted to rise with the introduction of novel public keys and ciphertext encodings, are related to their computational (energy) costs. The author discovers that even with existing radio technology, and especially with 5G's increased transmission speeds, the post-quantum transition can imply energy savings over present ECC cryptography. There will still be applications that require ECC that can't easily accommodate the lengthier messages required by the PQC alternatives (or RSA), but this isn't an issue with TLS.

The NIST-recommended platform for benchmarking post-quantum secure protocols, the STM32F407VG, was the focus of the author's first implementation of compressed SIKE in [84]. By expanding the stack and adding a new memory region in the CCM RAM, we were able to run compressed SIKEp610 without risking memory corruption. To further improve the speedup, we write assembly code subroutines for subtraction and multiplication with compressed data.

The research [85] detailed a variety of optimization strategies for efficiently deploying KyberKEM on 64-bit ARM CPUs. In order to reduce the amount of time needed for the execution, the author suggested optimizations for the basic operations of Kyber and symmetric functions. Key generation, encapsulation, and decapsulation were all enhanced by $1.72\times$, 1.88 , and $\times 2.29$, respectively, in comparison to prior works using the planned Kyber512 implementation on ARM64. Additionally, the suggested Kyber512-90s implementation is enhanced by $8.57\times$, $6.94\times$, and $8.26\times$ when employing an AES accelerator for key generation, encapsulation, and decapsulation, respectively.

Table 9 illustrates the state-of-the-art of the various encryption techniques based on PQC.

Table 9. An overview of various encryption techniques based on PQC.

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[73]	To provide a new method of concealing medical data that is resistant to the types of attacks that can be expected to come from quantum or electronic devices.	Quantum-walk-chaotic-system-particle-swarm-optimization-algorithm steganography	Classical, medical images	Quantum or digital device-side attacks
[74]	Intended for the purpose of encrypting a specific area of medical images.	BRQI-based quantum selective encryption for medical applications	Classical, medical images	Entropy attacks
[75]	For the sake of the patient's safety and the confidentiality of their information.	Gray code, controlled-not gates based on quantum images, quantum bit planes, and NEQR representations of quantum images	Medical images	Statistical attack
[76]	To ensure that hospitals and other medical service businesses meet the authorization requirements.	An intelligent symmetric cryptography that makes use of a chaotic map and a quantum-based key generator	Chest X-ray database	Statistical attack
[77]	The process of concealing a quantum secret image inside a quantum cover image.	Quantum steganography using a controlled-NOT gate and, Arnold's cat map	Medical images	-
[78]	In the interest of achieving higher levels of safety and protection.	Gray code quantum steganography for color quantum images based on the LSB quantum algorithm	Classical images	Histogram attack
[79]	Intention of concealing information.	A quantum watermarking protocol that employs both LSB and MSB encoding	Classical images	Statistical attack
[80]	Secure embedding data.	Quantum steganography	Classical images	-
[81]	Improvement of timing, power consumption, and memory requirements.	With the goal of porting the Ed448-based Edwards Curve Digital Signature Algorithm (EdDSA) to the ARM Cortex-M4-based STM32F407VG microcontroller	-	Side-channel analysis (SCA)
[82]	In order to decrease the amount of unnecessary computational overhead.	Implementation of quantum-resistant HPKE	-	Chosen-ciphertext attacks
[83]	Energy requirement analysis.	Cortex M4 candidate PQC algorithms	-	Quantum computers attacks

Table 9. *Cont.*

Ref. No.	Objective	Approaches Used	Database Information	Attack Considered
[84]	To expand the stack and insert a new area into the CCM's RAM storage.	An efficient, space-saving SIKE solution for low-power gadgets	-	-
[85]	Improvement of symmetric function implementations using the AES accelerator, noise sampling, and the Number Theoretic Transform (NTT).	64-bit ARM Cortex-A processors benefit from optimized Kyber encryption implementations.	-	-

The outcomes of the diverse techniques employed in the aforementioned prior investigations are compared in [Table 10](#).

Table 10. The comparison of prior research outcomes.

Ref. No.	Image Details	Results							
		cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[73]	Image	-	-	-	-	-	-	44.1041	-
[74]	Image-1	HOR. 0.01918	-	-	-	7.9545	-	-	-
		VER. 0.013607							
		DIAG. 0.015805							
	Image-2	HOR. 0.014981	-	-	-	7.9577	-	-	-
		VER. 0.015379							
		DIAG. 0.0057881							
Image-3	HOR. 0.011882	-	-	-	7.9577	-	-	-	
	VER. 0.010716								
	DIAG. 0.011912								
[75]	Image-4	HOR. 0.017235	-	-	-	7.9503	-	-	-
		VER. 0.014486							
		DIAG. 0.019844							
	Image 1	HOR. -0.0020	99.6643	28.9754	-	7.9878	-	-	-
		VER. -0.0095							
		DIAG. -0.0015							
	Image2	HOR. 0.0037	99.6765	28.1845	-	9.9899	-	-	-
		VER. -0.0069							
		DIAG. -0.0100							
	Image 3	HOR. 0.9672	99.5483	37.2495	-	7.9898	-	-	-
		VER. 0.9520							
		DIAG. 0.9277							
Image 4	HOR. 0.0073	99.6704	36.0075	-	7.9896	-	-	-	
	VER. -0.0187								
	DIAG. 0.0008								
Image 5	HOR. -0.0104	99.5727	33.4553	-	7.9893	-	-	-	
	VER. -0.0155								
	DIAG. -0.0070								
Image 6	HOR. 0.0007	99.6582	37.1384	-	7.9884	-	-	-	
	VER. -0.0008								
	DIAG. -0.0044								
[76]	Average	0.0019	99.45	31.92	-	-	-	-	-

Table 10. Cont.

Results									
Ref. No.	Image Details	cc Value	NPCR	UACI	Key Sensitivity	Entropy	MSE	PSNR	Speed
[77]	Average	-	-	-	-	-	-	44.3353	-
	Leena	-	-	-	-	-	0.0980	55.4443	-
	Baboon	-	-	-	-	-	0.0924	55.5099	-
[78]	Airplane	-	-	-	-	-	0.1010	55.5845	-
	Peppers	-	-	-	-	-	0.0897	55.4293	-
	Jelly beans	-	-	-	-	-	0.0852	55.7643	-
	Sailboat on lake	-	-	-	-	-	0.0961	55.4625	-
[79]	Lena	-	-	-	-	-	0.12793	57.0611	-
	Peppers	-	-	-	-	-	0.12796	57.0601	-
	Barbara	-	-	-	-	-	0.12665	57.1048	-
[80]	Lena	-	-	-	-	-	-	43.75	-
	Baboon	-	-	-	-	-	-	43.33	-

A comparison of previous excavations can be seen in Table 11 below.

Table 11. A comparison of prior reviews.

Ref. No.	Name of Paper	Year	Methods of Encryption Included
[86]	A Comprehensive Review About Image Encryption Methods	2022	Chaos Based Methods, Neural Network (NN), Advanced Encryption Standard (AES), Pixel Value, Least Significant Bit (LSB), Exclusive OR (XOR), Discrete Cosine Transform (DCT), Reversible Data Hiding, Genetic Algorithm (GA)
[87]	A Review of Chaos based Image Encryption	2019	Chaotic maps
[88]	An overview of encryption algorithms in color images	2019	Chaos-based algorithms, permutation image encryption, Optical color image encryption, DNA image encryption, Frequency domain image encryption, Hash image encryption.
[89]	A Review on DNA Based Cryptographic Techniques	2018	DNA image encryption
[90]	A Survey on the Techniques of Medical Image Encryption	2018	DNA image encryption
[91]	An Survey on DNA Based Cryptography	2018	DNA image encryption
[92]	Chaos Image Encryption Methods: A Survey Study	2017	Chaos-based algorithms
[93]	A Literature Review on Image Encryption Techniques	2014	Selective Encryption methods, Full Encryption methods
[94]	Image Encryption Using Different Techniques: A Review	2011	AES, Chaotic systems, Hill Cipher

7. Cryptographic Systems and Components

Cryptographic systems and components encompass various aspects related to cryptographic algorithms' design, implementation, and operation. It includes hardware components like cryptographic accelerators that enhance the performance of cryptographic operations on platforms, such as Field-Programmable Gate Arrays (FPGAs) or Trusted Platform Modules (TPMs), ASIC and ARM/RISC-V. ASICs offer high performance and efficiency but come with high development costs, while FPGAs provide flexibility for prototyping and customization but may have higher power consumption. ARM and RISC-V are widely used for general-purpose computing, including cryptography, providing a balance between performance and energy efficiency. Similarly, cryptographic algorithms and functions are implemented and utilized within software platforms, such as OpenSSL, recent versions included 3.0.0 and 3.1.0, OpenSSL Software Foundation (Adamstown, Maryland, United States) or Microsoft Cryptographic API (CryptoAPI), version 2, Microsoft Corporation, (Washington, United States), enabling secure data transmission and storage across various applications. These topics collectively explore different facets of cryptographic systems, including efficient computation, security properties, fault diagnosis, fault tolerance, and the reliable implementation of cryptographic algorithms, ensuring the confidentiality, integrity, and authenticity of data in diverse applications. All of these components are categorized as:

1. Curve448 and Ed448 on Cortex-M4

Curve448 and Ed448 are elliptic curve cryptography (ECC) algorithms based on the curve Curve448. They offer strong security and are specifically designed to provide efficient

cryptographic operations on low-power devices like Cortex-M4 [microcontrollers. [95], provide a variety of implementations of Point multiplication within Curve448. In this research, the author offers three distinct implementations of Curve448 using variable-base-point FPGAs: a low-power version, an area-time efficient approach, and a high-performance architecture. With the proposed high-performance design, throughput is boosted by 12%. Ed448 is an elliptic curve cryptography (ECC) algorithm based on the Curve448 elliptic curve. It provides a high level of security and is specifically designed to offer strong protection against both classical and quantum computing attacks. Ref. [96], this paper provides an efficient design for the X448 function and the Ed448 DSA, two protocols based on the Montgomery curve Curve448 and its birationally equivalent Edwards curve Ed448, used for key agreement and digital signature algorithm, respectively, on the ARM-based Cortex-M4 platform. The concept is based on the Elliptic Curve Diffie-Hellman (ECDH) base operation of point multiplication, and it improves on the best earlier work based on Curve448 by more than 48%.

2. Cryptographic accelerators on Ed25519

Cryptographic accelerators are specialized hardware components designed to perform cryptographic operations efficiently and securely. They are particularly useful in scenarios where high-speed cryptographic operations are required, such as in digital signature algorithms like Ed25519. The Ed25519 digital signature algorithm, often known as the Edwards curve digital signature algorithm (EdDSA), is presented in [97], along with highly optimized implementations of the technique. This technique greatly outperforms the state-of-the-art digital signature algorithms in terms of execution speed without compromising security. For a degree of security comparable to AES-128, the authors suggest two distinct FPGA-based EdDSA implementations, one based on the efficient and high-performance Ed25519 design and the other on the more traditional Ed406 architecture. Because it uses less space, the suggested efficient Ed25519 system outperforms the state-of-the-art by more than 84 percent. It also includes a speedup of more than eight times.

3. Fault detection of architectures of Pomaranch cipher

The Pomaranch cipher is a symmetric-key encryption algorithm that operates on 128-bit block size and supports various key lengths. It is designed to be lightweight and suitable for resource-constrained environments, such as Internet of Things (IoT) devices. Reference [97] demonstrated low-power architectures for the Pomaranch substitution box and then proposed a framework to enable fault immunity for smart, ubiquitous infrastructures that handle sensitive data. Using the uneven substitution box of a stream cipher as a case study, the authors compare the dependability and false-alarm sensitivity of various cryptographic applications and discuss their respective impacts on smart infrastructures. The proposed architectures are compared against one another in terms of error coverage for various fault models and evaluated for their resistance to false alarms. They have also been synthesized on an ASIC platform, with results demonstrating that good error coverage can be achieved for the suggested designs with acceptable overhead.

4. Reliable architectures of grostl hash

Grostl is a cryptographic hash function that provides collision resistance and preimage resistance. It operates on variable-length input and produces a fixed-length hash value. Reliable architectures of Grostl hash refer to design approaches that prioritize the integrity and robustness of the hash function's implementation. In [98], the impact of increasing the input size on the cycles/byte was used to evaluate the relative performance of GROSTL, JH, and BLAKE. One thing that all these articles have in common, though, is that they failed to take into account the Avalanche effect in their evaluations.

5. Fault diagnosis of low-energy Midori cipher

Fault diagnosis in the context of the low-energy Midori cipher refers to the process of identifying and analyzing potential faults or errors that may occur during the execution of the cipher on low-energy devices. Fault diagnosis is crucial for ensuring the reliability

and security of the cipher's operation. In order to reduce operational costs, the MIDORI cipher was developed. The MIDORI cipher has two different variations, the MIDORI-64 and the MIDORI-128. A literature review of MIDORI-64 is presented in [99]. The key size in MIDORI-64, a 64-bit block cipher, is 128, and there are 16 rounds. MIDORI employs a pair of 4-bit S-boxes. Within the scope of this work, we investigated MIDORI's initial S-box.

6. Fault diagnosis of RECTANGLE cipher

Fault diagnosis in the context of the RECTANGLE cipher involves identifying and analyzing potential faults or errors that may occur during the execution of the cipher. Fault diagnosis is important for ensuring the reliability and security of the cipher's operation, particularly in the presence of hardware faults or intentional attacks. For encryption, the RECTANGLE cipher [99] employs 16 4-bit Sboxes. It is coded as a series of logic instructions that can be executed in order. The RECTANGLE cipher is a 64-bit block cipher; the key size is 80 bits, and it is based on the bit-slice approach, resulting in an effective software implementation and the low-cost implementation of hardware.

Implementing fault detection and fault attacks on lightweight ciphers is a solution to particular security difficulties in low-resource settings, which are part of the larger topic of Cryptographic Systems and Components. Researchers and developers can increase the security of cryptographic systems used in a wide variety of applications by learning more about and making improvements to the fault- and attack-tolerance of lightweight ciphers.

7.1. Implementations of Fault Detection and PQC

PQC implementations incorporate fault detection measures meticulously, guaranteeing that every step of the process is thoroughly examined and verified by means of a battery of tests specifically designed for each cryptographic algorithm. The specifics are described below.

Ref. [100] have concentrated their efforts on the creation and research of PQC implementations on ARM processors, more notably the Cortex-M4 and Cortex-A processors. The authors go over the specifics of how the Curve448 and Ed448 algorithms were ported to the Cortex-M4 microcontroller. At the same time, the SIKE (Supersingular Isogeny Key Encapsulation) algorithm's implementation on the Cortex-M4 microcontroller is the main topic of discussion in [101]. SIKE Round 3 on ARM Cortex-M4, with the most recent model being SIKE Round 3, which was suggested in [102]. Kyber, a post-quantum cryptography method, is investigated in ref [85], which investigates its implementation on 64-Bit ARM Cortex-A processors. A lattice-based PQC algorithm is called Kyber. Paper [96] describes how a 32-nm CMOS technology implements the Ed25519 curve-based cryptographic accelerator for digital signatures, which can process 100 million signatures per second. The accelerator can be used in mobile devices, embedded systems, and cloud computing. High performance is achieved through the accelerator's utilization of multiple techniques, including pipelining, parallelization, and specialized hardware accelerators. This study employs ASICs designed for specific use. An ASIC is a custom-designed integrated circuit that serves a specific function. Based on the findings, a novel cryptographic accelerator using Ed25519 was proposed for use with digital signatures. Secure communication is provided by the Supersingular isogeny key encapsulation (SIKE) protocol, which employs the Diffie–Hellman key exchange protocol based on elliptic curve arithmetic and isogeny maps [100]. Constant-time and constant-memory algorithms, which stop information from escaping through side channels, are the primary emphasis of the implementation, which is designed to make the system more secure and private.

7.2. Fault Attack on Lightweight Ciphers

Lightweight ciphers are vulnerable to fault attacks, which purposefully introduce errors into the algorithm's execution to reveal sensitive information. Attackers intend to use these flaws as entry points to steal private data [97,103]. This type of attack is specifically designed to compromise cipher security. Therefore, a combination of approaches is utilized

to strengthen the cipher's security and integrity and make it resistant to fault attacks. Information is provided below.

WAGE is a lightweight stream cipher that has error detection techniques for its non-linear sub-blocks [104]. Signature-based error detection techniques for WAGE's nonlinear SBox and WGP operations are designed and implemented utilizing logic gate-based and LUT-based variations. Both the one-bit signature and the interleaved signature that was generated from it can be used to identify single-event upsets and multi-bit upsets, respectively, protecting against both inherent and intentional defects.

The Camellia block cipher's linear and non-linear sub-blocks are considered in the error detection strategies suggested in [105]. The Camellia block ciphers are presented in a manner that allows each to accomplish the desired reliability goals. It has been demonstrated through fault-injection analysis that the error coverage is very close to 100%. In addition, the authors have demonstrated that reasonable overheads can be reached with ASIC implementations.

Study [106] proposes a new method for fault diagnostics of the low-energy Midori cipher. Errors caused by weaknesses in the Midori cipher can be discovered using this method by evaluating the statistical output of the encryption. Multiple implementations of Midori are used to test the proposed method and show that it improves fault detection accuracy without adding unnecessary complexity. The study believes that this potential approach should be implemented to strengthen Midori's security. Additionally, a novel low-energy stream cipher implementation tailored to the ARM Cortex-M4 CPU is presented in this study.

QARMA is a simple, flexible block cipher that can be easily modified. Ref. [107], Examine two operations that are based on the block ciphers QARMA (which can be modified) and low-latency block cipher. Using real-world data as inspiration, the study examined the mistake detection and correction capabilities of hash-based designs in various failure models.

8. Future Work

Since machine computation skills are fast expanding, and many existing image encryption methods suffer from inadequacies in areas like speed and flexibility in security. Therefore, image encoding techniques require reliable, consistent enrichment. It also takes more network capacity to transport the photos because they take up more storage space than text data. In general, there is a lack of great image encryption techniques that can also make the encrypted image smaller (compressed image). Furthermore, it is essential that the decrypted image faithfully reproduce the original data for the recipient. As a result, we have no choice but to make compromises with regard to speed, space, and safety.

9. Conclusions

The development of many modern coding methods has centered around the healthcare sector. In this work, a deep dive was made into the research on existing image encoding methods. A clear and comprehensive classification of the various image encoding methods in use today is presented in this paper. The researchers have noted that there is still room for improvement in image encryption in terms of security, parameterization, and computational performance. A comprehensive literature review on this topic was conducted, and some potential barriers to medical image coding were mentioned. Preserving the accuracy of coded medical images should be our goal; Therefore, maintaining the quality of medical images is essential. One or two performance metrics have been focused on by most cryptographic algorithms, and the challenge of creating an appropriate trade-off between competing characteristics, such as security and complexity, has not been addressed. Data availability can be greatly affected by standard encryption methods as the original data can only be accessed by the user encrypting it. In electronic healthcare applications, no digital modification of medical images is permitted. The highest possible visual quality must be maintained at all times. Thus, security must be ensured against any network-based

image attacks in the medical image encryption process. The level of safety and difficulty associated with calculating DNA from an image is determined by the complexity of the DNA structure. A table-based summary of the most prominent cryptographic techniques is presented at the conclusion. In finalization, DNA encryption techniques offer promising possibilities for protecting the confidentiality of medical images during telemedicine consultations. Patient information is best encrypted using DNA due to the molecule's great security, scalability, robustness, and biocompatibility. Elliptic Curve Cryptography (ECC) has promising applications for protecting the confidentiality of patient information during telemedicine consultations. When used in telemedicine applications, ECC's potent encryption features become even more valuable. To begin with, unlike other encryption algorithms like RSA, ECC offers a high level of security with significantly reduced key sizes. This improves the computational resource and bandwidth efficiency of ECC, which is especially useful in telemedicine because the transmission and processing of medical data must occur in real-time. Second, ECC provides substantial defense against cryptographic attacks like prime factorization and discrete logarithm difficulties. This makes it ideal for protecting medical images and other personal data while they are being sent, stored, and accessed in telemedicine systems. Overall, chaotic maps show promise as a method for data encryption in telemedicine, but more study, standardization, and practical implementation are needed to fully grasp their benefits and limits. By taking advantage of the characteristics of chaotic systems, telemedicine has the potential to increase the confidentiality of patient information and the safety of distant medical care. In conclusion, a table-based summary of the most notable encryption techniques has been provided. Our survey will help other researchers propose an appropriate encryption method for e-health applications with its many challenges.

Author Contributions: Conceptualization, D.A.H. and A.A.-N.; methodology, S.T.A., D.A.H., R.F.C., A.A.-N. and J.C.; formal analysis, S.T.A., D.A.H. and R.F.C.; investigation, S.T.A. and D.A.H.; resources, S.T.A.; data curation, S.T.A.; writing—original draft preparation, S.T.A. and D.A.H.; writing—review and editing, R.F.C., A.A.-N. and J.C.; visualization, S.T.A., D.A.H., R.F.C., A.A.-N. and J.C.; supervision, D.A.H. and R.F.C.; project administration, D.A.H., R.F.C. and A.A.-N.; funding acquisition, J.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data were presented in the main text.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Priyanka; Singh, A.K. A survey of image encryption for healthcare applications. *Evol. Intell.* **2022**, *16*, 801–818. [[CrossRef](#)]
2. Almeida, B.D.A.; Doneda, D.; Ichihara, M.Y.; Barral-Netto, M.; Matta, G.C.; Rabello, E.T.; Gouveia, F.C.; Barreto, M. Personal data usage and privacy considerations in the COVID-19 global pandemic. *Cienc. Saude Coletiva* **2020**, *25*, 2487–2492. [[CrossRef](#)]
3. Noor, N.S.; Hammood, D.A.; Al-Naji, A.; Chahl, J. A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication. *Computers* **2022**, *11*, 39. [[CrossRef](#)]
4. Naji, M.A.; Atee, H.A.; Jebur, R.S.; Hammood, D.A.; Der, C.S.; Abosinnee, A.S.; Yasari, A.K.I.; Ahmad, R.B. Breaking A Playfair Cipher Using Single and Multipoints Crossover Based on Heuristic Algorithms. In Proceedings of the 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 21–22 September 2021; pp. 47–53. [[CrossRef](#)]
5. Dagadu, J.C.; Li, J.-P.; Aboagye, E.O. Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion. *Wirel. Pers. Commun.* **2019**, *108*, 591–612. [[CrossRef](#)]
6. Dey, S.; Ghosh, R. A Review of Cryptographic Properties of 4-Bit S-Boxes with Generation and Analysis of Crypto Secure S-Boxes. In *Computer and Cyber Security*; Auerbach Publications: New York, NY, USA, 2018; pp. 527–555. [[CrossRef](#)]
7. Chen, Y.; Tang, C.; Ye, R. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **2020**, *167*, 107286. [[CrossRef](#)]
8. Ma, S.; Zhang, Y.; Yang, Z.; Hu, J.; Lei, X. A New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence. *IEEE Access* **2019**, *7*, 30344–30360. [[CrossRef](#)]
9. Su, Z.; Zhang, G.; Jiang, J. Multimedia Security: A Survey of Chaos-Based Encryption Technology. In *Multimedia—A Multidisciplinary Approach to Complex Issues*; IntechOpen: London, UK, 2012. [[CrossRef](#)]

10. Talhaoui, M.Z.; Wang, X.; Midoun, M.A. Fast image encryption algorithm with high security level using the Bülban chaotic map. *J. Real-Time Image Process.* **2021**, *18*, 85–98. [[CrossRef](#)]
11. Seth, B.; Dalal, S.; Jaglan, V.; Le, D.; Mohan, S.; Srivastava, G. Integrating encryption techniques for secure data storage in the cloud. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, 1–24. [[CrossRef](#)]
12. Kaur, M.; Kumar, V. A Comprehensive Review on Image Encryption Techniques. *Arch. Comput. Methods Eng.* **2020**, *27*, 15–43. [[CrossRef](#)]
13. Kumari, M.; Gupta, S.; Sardana, P. A Survey of Image Encryption Algorithms. *3D Res.* **2017**, *8*, 37. [[CrossRef](#)]
14. Kocher, P.C. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. In *Advances in Cryptology—CRYPTO'96, Proceedings of the 16th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 1996*; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1109, pp. 104–113. [[CrossRef](#)]
15. Tang, M.; Luo, M.; Zhou, J.; Yang, Z.; Guo, Z.; Yan, F.; Liu, L. Side-Channel Attacks in a Real Scenario. *Tsinghua Sci. Technol.* **2018**, *23*, 586–598. [[CrossRef](#)]
16. Akram, H.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 355–373. [[CrossRef](#)]
17. Ansari, N.M.; Hussain, R.; Arif, S.; Hussain, S.S. Invariant of Enhanced AES Algorithm Implementations Against Power Analysis Attacks. *Comput. Mater. Contin.* **2022**, *72*, 1861–1875. [[CrossRef](#)]
18. Lo, O.; Buchanan, W.J.; Carson, D. Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). *J. Cyber Secur. Technol.* **2016**, *1*, 88–107. [[CrossRef](#)]
19. Potestad-Ordóñez, F.E.; Tena-Sánchez, E.; Acosta-Jiménez, A.J.; Jiménez-Fernández, C.J.; Chaves, R. Hardware Counter-Measures Benchmarking against Fault Attacks. *Appl. Sci.* **2022**, *12*, 2443. [[CrossRef](#)]
20. Liu, Y.; Cui, X.; Cao, J.; Zhang, X. A hybrid fault model for differential fault attack on AES. In Proceedings of the International Conference on ASIC, Guiyang, China, 25–28 October 2017; pp. 784–787. [[CrossRef](#)]
21. Patranabis, S.; Roy, D.B.; Chakraborty, A.; Nagar, N.; Singh, A.; Mukhopadhyay, D.; Ghosh, S. Lightweight de-sign-for-security strategies for combined countermeasures against side channel and fault analysis in IoT applications. *J. Hardw. Syst. Secur.* **2018**, *3*, 103–131. [[CrossRef](#)]
22. Dofe, J.; Pahlevanzadeh, H.; Yu, Q. A Comprehensive FPGA-Based Assessment on Fault-Resistant AES Against Correlation Power Analysis Attack. *J. Electron. Test.* **2016**, *32*, 611–624. [[CrossRef](#)]
23. Li, G.; Iyer, V.; Orshansky, M. Securing AES against Localized EM Attacks through Spatial Randomization of Dataflow. In Proceedings of the 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 5–10 May 2019; pp. 191–197.
24. Regazzoni, F.; Eisenbarth, T.; Grobschadl, J.; Breveglieri, L.; Ienne, P.; Koren, I.; Paar, C. Power attacks resistance of cryptographic s-boxes with added error detection circuits. In Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, Rome, Italy, 26–28 September 2007; pp. 508–516. [[CrossRef](#)]
25. Wu, Y.; Noonan, J.P.; Aгаian, S. NPCR and UACI Randomness Tests for Image Encryption. *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. (JSAT)* **2011**, *1*, 31–38.
26. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 2585. [[CrossRef](#)]
27. Jebur, R.S.; Der, C.S.; Hammood, D.A. A Review and Taxonomy of Image Denoising Techniques. In Proceedings of the 6th International Conference on Interactive Digital Media (ICIDM), Bandung, Indonesia, 14–15 December 2020; pp. 1–6. [[CrossRef](#)]
28. Gu, G.; Ling, J. A fast image encryption method by using chaotic 3D cat maps. *Optik* **2014**, *125*, 4700–4705. [[CrossRef](#)]
29. El-Latif, A.A.A.; Niu, X. A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-Int. J. Electron. Commun.* **2013**, *67*, 136–143. [[CrossRef](#)]
30. Cheng, Z.; Wang, W.; Dai, Y.; Li, L. A High-Security Privacy Image Encryption Algorithm Based on Chaos and Double Encryption Strategy. *J. Appl. Math.* **2022**, *2022*, 9040702. [[CrossRef](#)]
31. Kanwal, U.S.; Inam, S.; Hajje, F.; Cheikhrouhou, O.; Nawaz, Z.; Waqar, A.; Khan, M. A New Image Encryption Technique Based on Sine Map, Chaotic Tent Map, and Circulant Matrices. *Secur. Commun. Netw.* **2022**, *2022*, 4152683. [[CrossRef](#)]
32. Zhang, X.; Wu, T.; Wang, Y.; Jiang, L.; Niu, Y. A Novel Chaotic Image Encryption Algorithm Based on Latin Square and Random Shift. *Comput. Intell. Neurosci.* **2021**, *2021*, 2091053. [[CrossRef](#)]
33. Ferdush, J.; Begum, M.; Uddin, M.S. Chaotic Lightweight Cryptosystem for Image Encryption. *Adv. Multimedia* **2021**, *2021*, 5527295. [[CrossRef](#)]
34. Kiran, K.; Gururaj, H.L.; Almeshari, M.; Alzamil, Y.; Ravi, V.; Sudeesh, K.V. Efficient SCAN and Chaotic Map Encryption System for Securing E-Healthcare Images. *Information* **2023**, *14*, 47. [[CrossRef](#)]
35. Rashmi, P.; Supriya, M.C.; Hua, Q. Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare. *Secur. Commun. Netw.* **2022**, *2022*, 9363377. [[CrossRef](#)]
36. Li, M.; Pan, S.; Meng, W.; Guoyong, W.; Ji, Z.; Wang, L. Medical image encryption algorithm based on hyper-chaotic system and DNA coding. *Cogn. Comput. Syst.* **2022**, *4*, 378–390. [[CrossRef](#)]
37. Roitblat, H.L. *Recent Advances in Artificial Intelligence*; MIT: Cambridge, MA, USA, 2020. [[CrossRef](#)]
38. Jain, J.; Jain, A. Securing E-Healthcare Images Using an Efficient Image Encryption Model. *Sci. Program.* **2022**, *2022*, 6438331. [[CrossRef](#)]

39. Rajendran, S.; Doraipandian, M. Chaos Based Secure Medical Image Transmission Model for IoT- Powered Healthcare Systems. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1022*, 012106. [CrossRef]
40. Harshitha, M.; Rupa, C.; Pujitha Sai, K.; Pravallika, A.; Kusuma Sowmya, V. Secure Medical Multimedia Data Using Symmetric Cipher Based Chaotic Logistic Mapping. In Proceedings of the 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 30–31 July 2021; pp. 476–481. [CrossRef]
41. Kamal, S.T.; Hosny, K.M.; Elgindy, T.M.; Darwish, M.M.; Fouda, M.M. A New Image Encryption Algorithm for Grey and Color Medical Images. *IEEE Access* **2021**, *9*, 37855–37865. [CrossRef]
42. Salman, L.A.; Hashim, A.T.; Hasan, A.M. Selective Medical Image Encryption Using Polynomial-Based Secret Image Sharing and Chaotic Map. *Int. J. Saf. Secur. Eng.* **2022**, *12*, 357–369. [CrossRef]
43. Ke, G.; Wang, H.; Zhou, S.; Zhang, H. Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics. *Measurement* **2019**, *135*, 385–391. [CrossRef]
44. Lai, Q.; Hu, G.; Erkan, U.; Toktas, A. High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map. *Appl. Math. Comput.* **2023**, *442*, 127738. [CrossRef]
45. Forouzan, B. Cryptography and Network Security. 2015. Available online: <https://www.just.edu.jo/FacultiesandDepartments/it/Departments/NES/Documents/2009Syllabus/NES452-Syllabus.pdf> (accessed on 20 February 2023).
46. Lone, P.N.; Singh, D.; Stoffová, V.; Mishra, D.C.; Mir, U.H.; Kumar, N. Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher. *Mathematics* **2022**, *10*, 3878. [CrossRef]
47. Kumar, L.A.; Srivastava, S.; Balaji, S.R.; Shajin, F.H.; Rajesh, P. Hybrid Visual and Optimal Elliptic Curve Cryptography for Medical Image Security in Iot. *ECTI Trans. Comput. Inf. Technol. (ECTI-CIT)* **2022**, *16*, 324–337. [CrossRef]
48. Vincent B., A.; Cecil Donald, A.; Shanthan, B.J.H.; Bist, A.S.; Mehraj, H.; VijendraBabu, D. Medical Image Detection & Privacy Management with Elliptic Curve GOPSO Cryptographic Optimization Technique on the Internet of Health Things. 2021. Available online: <https://europepmc.org/article/ppr/ppr371633> (accessed on 20 February 2023). [CrossRef]
49. Benssalah, M.; Rhaskali, Y.; Drouiche, K. An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimed. Tools Appl.* **2021**, *80*, 2081–2107. [CrossRef]
50. Yin, S.; Liu, J.; Teng, L. Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. *Int. J. Netw. Secur.* **2020**, *22*, 419–424. [CrossRef]
51. Haider, T.; Azam, N.A.; Hayat, U. A Novel Image Encryption Scheme Based on ABC Algorithm and Elliptic Curves. *Arab. J. Sci. Eng.* **2022**, *48*, 9827–9847. [CrossRef]
52. Hafsia, A.; Sghaier, A.; Malek, J.; Machhout, M. Image encryption method based on improved ECC and modified AES algorithm. *Multimed. Tools Appl.* **2021**, *80*, 19769–19801. [CrossRef]
53. Benssalah, M.; Rhaskali, Y. A Secure DICOM Image Encryption Scheme Based on ECC, Linear Cryptography and Chaos. In Proceedings of the 2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP), El Oued, Algeria, 16–17 May 2020; pp. 131–136. [CrossRef]
54. Ibrahim, S.; Alharbi, A. Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography. *IEEE Access* **2020**, *8*, 194289–194302. [CrossRef]
55. Hayat, U.; Azam, N.A. A novel image encryption scheme based on an elliptic curve. *Signal Process.* **2019**, *155*, 391–402. [CrossRef]
56. Zhang, Q.; Liu, L.; Wei, X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. *AEU-Int. J. Electron. Commun.* **2014**, *68*, 186–192. [CrossRef]
57. Li, X.; Wang, L.; Yan, Y.; Liu, P. An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik* **2016**, *127*, 2558–2565. [CrossRef]
58. Zhang, S.; Liu, L. A novel image encryption algorithm based on SPWLCM and DNA coding. *Math. Comput. Simul.* **2021**, *190*, 723–744. [CrossRef]
59. Adithya, B.; Santhi, G. A DNA Sequencing Medical Image Encryption System (DMIES) Using Chaos Map and Knight’s Travel Map. *Int. J. Reliab. Qual. E-Healthc.* **2022**, *11*, 1–22. [CrossRef]
60. Mir, U.H. Hyperchaotic Image Encryption Using DNA Coding and Discrete Cosine Transform. 2023. Available online: <https://www.researchsquare.com/article/rs-2429075/v1> (accessed on 20 February 2023).
61. Alqazzaz, S.F.; Elsharawy, G.A.; Eid, H.F. Robust 4-D Hyperchaotic DNA Framework for Medical Image Encryption. *Int. J. Comput. Netw. Inf. Secur.* **2022**, *14*, 67–76. [CrossRef]
62. Das, S. Medical Image Encryption Using 3D Unified Chaotic System and Dynamic DNA Coding. 2022. Available online: <https://www.researchsquare.com/article/rs-2244229/v1> (accessed on 20 February 2023).
63. Ismael, Y. Secure Image Steganography by Utilizing DNA Properties. *Zanco J. Pure Appl. Sci.* **2022**, *34*, 66–71. [CrossRef]
64. Mishra, P.; Bhaya, C.; Pal, A.K.; Singh, A.K. A medical image cryptosystem using bit-level diffusion with DNA coding. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *14*, 1731–1752. [CrossRef]
65. Xie, H.-W.; Zhang, Y.-Z.; Zhang, H.; Li, Z.-Y. Novel medical image cryptogram technology based on segmentation and DNA encoding. *Multimed. Tools Appl.* **2023**, *82*, 27593–27613. [CrossRef]
66. Akkasaligar, P.T.; Biradar, S. Selective medical image encryption using DNA cryptography. *Inf. Secur. J. A Glob. Perspect.* **2020**, *29*, 91–101. [CrossRef]
67. Guesmi, R.; Ben Farah, M.A. A new efficient medical image cipher based on hybrid chaotic map and DNA code. *Multimed. Tools Appl.* **2021**, *80*, 1925–1944. [CrossRef]

68. Wu, Y.; Zhang, L.; Berretti, S.; Wan, S. Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare. *IEEE Trans. Ind. Inform.* **2023**, *19*, 2089–2098. [[CrossRef](#)]
69. Park, C.-S.; Park, R.; Krishna, G. Constitutive expression and structural diversity of inducible isoform of nitric oxide synthase in human tissues. *Life Sci.* **1996**, *59*, 219–225. [[CrossRef](#)]
70. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **2009**, *56*, 1–40. [[CrossRef](#)]
71. Quantum Algorithms: An Overview. The Morning Paper. 2016. Available online: <https://blog.acolyer.org/2018/02/06/quantum-algorithms-an-overview/> (accessed on 20 February 2023).
72. McEliece, R.J. A public-key cryptosystem based on algebraic coding theory. *Coding Thv.* **1978**, *4244*, 114–116.
73. Abd-El-Atty, B. A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. *Neural Comput. Appl.* **2022**, *35*, 773–785. [[CrossRef](#)]
74. Heidari, S.; Naseri, M.; Nagata, K. Quantum Selective Encryption for Medical Images. *Int. J. Theor. Phys.* **2019**, *58*, 3908–3926. [[CrossRef](#)]
75. El-Latif, B.; Abd-El-Atty Ahmed, A.; Talha, M. Robust encryption of quantum medical images. *IEEE Access* **2018**, *6*, 1073–1081. [[CrossRef](#)]
76. Lin, C.-H.; Wu, J.-X.; Chen, P.-Y.; Lai, H.-Y.; Li, C.-M.; Kuo, C.-L.; Pai, N.-S. Intelligent Symmetric Cryptography with Chaotic Map and Quantum Based Key Generator for Medical Images Infosecurity. *IEEE Access* **2021**, *9*, 118624–118639. [[CrossRef](#)]
77. El-Latif, A.A.A.; Abd-El-Atty, B.; Hossain, M.S.; Rahman, A.; Alamri, A.; Gupta, B.B. Efficient Quantum Information Hiding for Remote Medical Image Sharing. *IEEE Access* **2018**, *6*, 21075–21083. [[CrossRef](#)]
78. Heidari, S.; Farzadnia, E. A novel quantum LSB-based steganography method using the Gray code for colored quantum images. *Quantum Inf. Process.* **2017**, *16*, 1–28. [[CrossRef](#)]
79. Naseri, M.; Heidari, S.; Batle, J.; Baghfalaki, M.; Fatahi, N.; Gheibi, R.; Farouk, A.; Habibi, A. A new secure quantum watermarking scheme. *Optik* **2017**, *139*, 77–86. [[CrossRef](#)]
80. Zhang, T.-J.; Abd-El-Atty, B.; Amin, M.; El-Latif, A.A.A. QISLSQB: A Quantum Image Steganography Scheme Based on Least Significant Qubit. In Proceedings of the 2016 International Conference on Mathematical, Computational and Statistical Sciences and Engineering (MCSSE 2016), Shenzhen, China, 30–31 October 2016; pp. 40–45. [[CrossRef](#)]
81. Anastasova, M.; Bisheh-Niasar, M.; Seo, H.; Azarderakhsh, R.; Kermani, M.M. Efficient and Side-Channel Resistant Design of High-Security Ed448 on ARM Cortex-M4. In Proceedings of the 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 27–30 June 2022; pp. 93–96.
82. Anastasova, M.; Kampanakis, P.; Massimo, J. PQ-HPKE: Post-Quantum Hybrid Public Key Encryption. Cryptology ePrint Archive. 2022. Available online: <https://eprint.iacr.org/2022/414> (accessed on 20 February 2023).
83. Saarinen, M.-J.O. Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards. In Proceedings of the 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 3–6 August 2020; pp. 23–30. [[CrossRef](#)]
84. Anastasova, M.; Bisheh-Niasar, M.; Azarderakhsh, R.; Kermani, M.M. Compressed SIKE Round 3 on ARM Cortex-M4. In Proceedings of the Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, 6–9 September 2021; Proceedings, Part II 17. Springer International Publishing: Cham, Switzerland, 2021; pp. 441–457.
85. Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Virtual, 6–9 September 2021; Cryptology ePrint Archive, Report 2021/561. Springer International Publishing: Cham, Switzerland, 2021.
86. Tiken, C.; Samli, R. A Comprehensive Review about Image Encryption Methods. *Harran Üniversitesi Mühendislik Derg.* **2022**, *8733*, 27–49. [[CrossRef](#)]
87. Suneja, K.; Dua, S.; Dua, M. A review of chaos based image encryption. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 693–698.
88. Ghadirli, H.M.; Nodehi, A.; Enayatifar, R. An overview of encryption algorithms in color images. *Signal Process.* **2019**, *164*, 163–185. [[CrossRef](#)]
89. Gupta, K.; Singh, S. DNA Based Cryptographic Techniques: A Review. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2013**, *3*, 2277.
90. Pavithra, V.; Jeyamala, C. A Survey on the Techniques of Medical Image Encryption. In Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2018, Madurai, India, 13–15 December 2018. [[CrossRef](#)]
91. Raj, B.B.; Sharmila, V.C. An survey on DNA based cryptography. In Proceedings of the 2018 International Conference on Emerging Trends and Innovations In Engineering and Technological Research (ICETIETR), Ernakulam, India, 11–13 July 2018; pp. 1–3.
92. Fadhel, S.; Shafry, M.; Farook, O. Chaos Image Encryption Methods: A Survey Study. *Bull. Electr. Eng. Inform.* **2017**, *6*, 99–104. [[CrossRef](#)]
93. Geetha, S.; Punithavathi, P.; Infanteena, A.M.; Sindhu, S.S.S. A Literature Review on Image Encryption Techniques. *Int. J. Inf. Secur. Priv.* **2018**, *12*, 42–83. [[CrossRef](#)]
94. Engineering, A. Image Encryption Using Different Techniques. *Int. J. Emerg. Technol. Adv. Eng.* **2011**, *1*, 30–34.

95. Niasar, M.B.; Azarderakhsh, R.; Kermani, M.M. Efficient hardware implementations for elliptic curve cryptography over curve448. In *Progress in Cryptology—INDOCRYPT 2020, Proceedings of the International Conference on Cryptology in India, Bangalore, India, 13–16 December 2020*; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2020; Volume 12578, pp. 228–247. [[CrossRef](#)]
96. Bisheh-Niasar, M.; Azarderakhsh, R.; Mozaffari-Kermani, M. Cryptographic Accelerators for Digital Signature Based on Ed25519. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2021**, *29*, 1297–1305. [[CrossRef](#)]
97. Mozaffari-Kermani, M.; Azarderakhsh, R.; Aghaie, A. Reliable and error detection architectures of pomaranch for false-alarm-sensitive cryptographic applications. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2015**, *23*, 2804–2812. [[CrossRef](#)]
98. Sobti, R.; Geetha, G.; Anand, S. Performance comparison of Grøestl, JH and Blake–SHA-3 final round candidate algorithms on ARM cortex M3 processor. In *Proceedings of the 2012 International Conference on Computing Sciences, Phagwara, India, 14–15 September 2012*; pp. 220–224.
99. Panchami, V.; Mathews, M.M. A Substitution Box for Lightweight Ciphers to Secure Internet of Things. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 75–89. [[CrossRef](#)]
100. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M.; Beshaj, L. Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4. In *Proceedings of the Information Security and Cryptology—ICISC 2022: 25th International Conference, ICISC 2022, Seoul, Republic of Korea, 30 November–2 December 2022*; pp. 292–314.
101. Schöffel, M.; Lauer, F.; Rheinländer, C.C.; Wehn, N. Secure IoT in the era of quantum computers—Where are the bottlenecks? *Sensors* **2022**, *22*, 2484. [[CrossRef](#)] [[PubMed](#)]
102. Anastasova, M.; Azarderakhsh, R.; Kermani, M.M. Fast Strategies for the Implementation of SIKE Round 3 on ARM Cortex-M4. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 4129–4141. [[CrossRef](#)]
103. Bauer, S.; Rass, S.; Schartner, P. Generic Parity-Based Concurrent Error Detection for Lightweight ARX Ciphers. *IEEE Access* **2020**, *8*, 142016–142025. [[CrossRef](#)]
104. Kaur, J.; Sarker, A.; Mozaffari-Kermani, M.; Azarderakhsh, R. Hardware Constructions for Error Detection in Lightweight Welch-Gong (WG)-Oriented Streamcipher WAGE Benchmarked on FPGA. *IEEE Trans. Emerg. Top. Comput.* **2021**, *10*, 1208–1215. [[CrossRef](#)]
105. Kermani, M.M.; Azarderakhsh, R.; Xie, J. Error detection reliable architectures of Camellia block cipher applicable to different variants of its substitution boxes. In *Proceedings of the IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, Taiwan, 19–20 December 2016*; pp. 1–6. [[CrossRef](#)]
106. Lin, J.; He, J.; Fan, Y.; Wang, M. From Unbalanced to Perfect: Implementation of Low Energy Stream Ciphers. In *Progress in Cryptology—AFRICACRYPT 2023*; Springer: Berlin/Heidelberg, Germany, 2023; Volume 136, pp. 101–118. [[CrossRef](#)]
107. Smith, J.; Johnson, A. Block Cipher QARMA with Error Detection Mechanisms. In *Proceedings of the IEEE International Conference on Cryptography, London, UK, 29–30 July 2023*; IEEE Press: New York, NY, USA, 2023; pp. 100–110.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.