mathematics

Review

Chaos-Based Image Encryption: Review, Application, and Challenges

Bowen Zhang and Lingfeng Liu *

School of Software, Nanchang University, Nanchang 330031, China; zhangbw94@email.ncu.edu.cn
* Correspondence: lfliu@ncu.edu.cn

Abstract: Chaos has been one of the most effective cryptographic sources since it was first used in image-encryption algorithms. This paper closely examines the development process of chaos-based image-encryption algorithms from various angles, including symmetric and asymmetric algorithms, block ciphers and stream ciphers, and integration with other technologies. The unique attributes of chaos, such as sensitivity to initial conditions, topological transitivity, and pseudo-randomness, are conducive to cross-referencing with other disciplines and improving image-encryption methods. Additionally, this paper covers practical application scenarios and current challenges of chaotic image encryption, thereby encouraging researchers to continue developing and complementing existing situations, and may also serve as a basis of future development prospects for chaos-based image encryption.

Keywords: chaos; image encryption; chaotic system; chaos-based image encryption; chaotic map; cryptography

MSC: 94A08; 94A60

check for updates

Citation: Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 2585. https://doi.org/10.3390/math11112585

Academic Editor: Jonathan Blackledge

Received: 8 May 2023
Revised: 1 June 2023
Accepted: 4 June 2023
Published: 5 June 2023

1. Introduction

1.1. A Brief Introduction to Chaos-Based Cryptography

Chaos is a pseudo-random and unpredictable motion exhibited in a deterministic dynamical system due to its sensitivity to initial values and parameters. The study of chaos theory originated from the three-body problem studied by H. Poincare in 1913. After various studies, E. N. Lorenz [1] proposed the Lorenz equation in 1963, which was the first example of a chaotic solution derived from a deterministic equation in a dissipative system. The term "chaos" was first used by Tienyien Li and James A. Yorke [2] in their 1975 paper "Period Three Implies Chaos" to describe this phenomenon. In 1976, Robert M. May [3] proposed the Logistic map in an article, which was studied in depth by M.J. Feigenbaum, who proposed the universality of this map in 1978. Since then, the study of chaos has developed vigorously.

A chaotic system is a complex and highly dynamic system, which is characterized by sensitivity to initial conditions, nonlinearity, aperiodicity, etc. The study of chaotic systems has become an important topic in the field of nonlinear dynamics because of their complex behavior, which is difficult to predict and control. Chaotic systems have a wide range of applications in many fields. In finance, chaotic systems are used to model the behavior of financial markets and to develop trading strategies. In biology, chaotic systems are used to study population dynamics and the behavior of biological systems. In neural networks, chaotic systems are used to model the behavior of neurons and to develop new algorithms for machine learning and artificial intelligence. In addition, chaotic systems are frequently employed in cryptography to develop secure communication systems, owing to their innate structural resemblances [4,5]. Robert Matthews [6] explicitly proposed the "chaotic encryption" algorithm in 1989. Since then, researchers have studied how systems change from ordered to chaotic states and the properties of chaotic systems. In the following years, there has been extensive research on chaos-based cryptography, which has also entered the practical application stage.

1.2. A Brief Introduction to Image Encryption

The network processing and dissemination of a large number of pictures can easily cause the disclosure of personal privacy information in the current era of rapid development of the Internet. Therefore, it is necessary to take some measures to encrypt and protect images. The data of an image has special characteristics, such as a large capacity, high redundancy, and high correlation between pixels; therefore, image encryption has special structural requirements. Image encryption is a technique that transforms image data into a cryptic form to safeguard image privacy and security. Encryption algorithms are commonly employed to obscure an image, making it arduous for unauthorized individuals to comprehend. Image encryption is mandatory to ensure the security of confidential images, including but not limited to personal, trade, and government secrets. Specifically, in digital image processing, image encryption functions by obstructing access to images, deterring theft or tampering by unauthorized entities. Image encryption can also be applied to digital watermarks and copyright information to preserve them. Moreover, it is essential to acknowledge that while image encryption mitigates security threats, it does not entirely prevent breaching or tampering. As a result, the security and reliability of image-encryption algorithms are critical for realizing comprehensive image encryption. In order to achieve this goal, more and more encryption algorithms based on different technologies have been proposed for image encryption, such as chaos-based encryption [7,8], S-Box-based encryption [9,10], optical encryption [11], compression encryption [12], frequency-domain-based encryption, and DNA-based encryption. This paper mainly introduces the chaos-based image-encryption scheme.

1.3. A Brief Introduction to Chaos-Based Image Encryption

Image data usually require more storage space than text data, and are characterized by high redundancy and high correlation between adjacent pixels. Therefore, traditional encryption methods cannot fulfill the demands for image encryption. However, utilizing chaos theory in image encryption provides a new approach. Chaotic systems are highly sensitive to initial conditions, and even small errors in the initial conditions can lead to vastly different motion trajectories. Although the chaotic trajectory is controlled when the initial conditions are determined, it is impossible to predict the trajectory over a long period without knowing the initial conditions. Additionally, chaotic systems have other features, including high ergodicity, determination, and pseudo-randomness, which are crucial for image encryption.

In recent years, scholars have applied different chaotic systems, including discrete chaotic maps and continuous chaotic systems, in image encryption to ensure the security of image transmission. In the next section, we cover these approaches in more detail.

The rest of this article is organized as shown in Figure 1. Section 2 provides an introduction to chaotic systems and their characteristics. Section 3 discusses the development of chaos-based image-encryption algorithms over the years, including symmetric and asymmetric chaotic algorithms, and chaotic algorithms combined with other technologies. A timeline of chaotic encryption algorithms with outstanding contributions is reviewed in this section. In Section 4, the security evaluation methods used for image-encryption algorithms are presented. Section 5 focuses on the application of chaos-based image-encryption algorithms in the medical, Internet of Things, and satellite fields. Section 6 addresses the current challenges and future research directions for chaos-based image encryption. Finally, Section 7 provides a summary of this article.

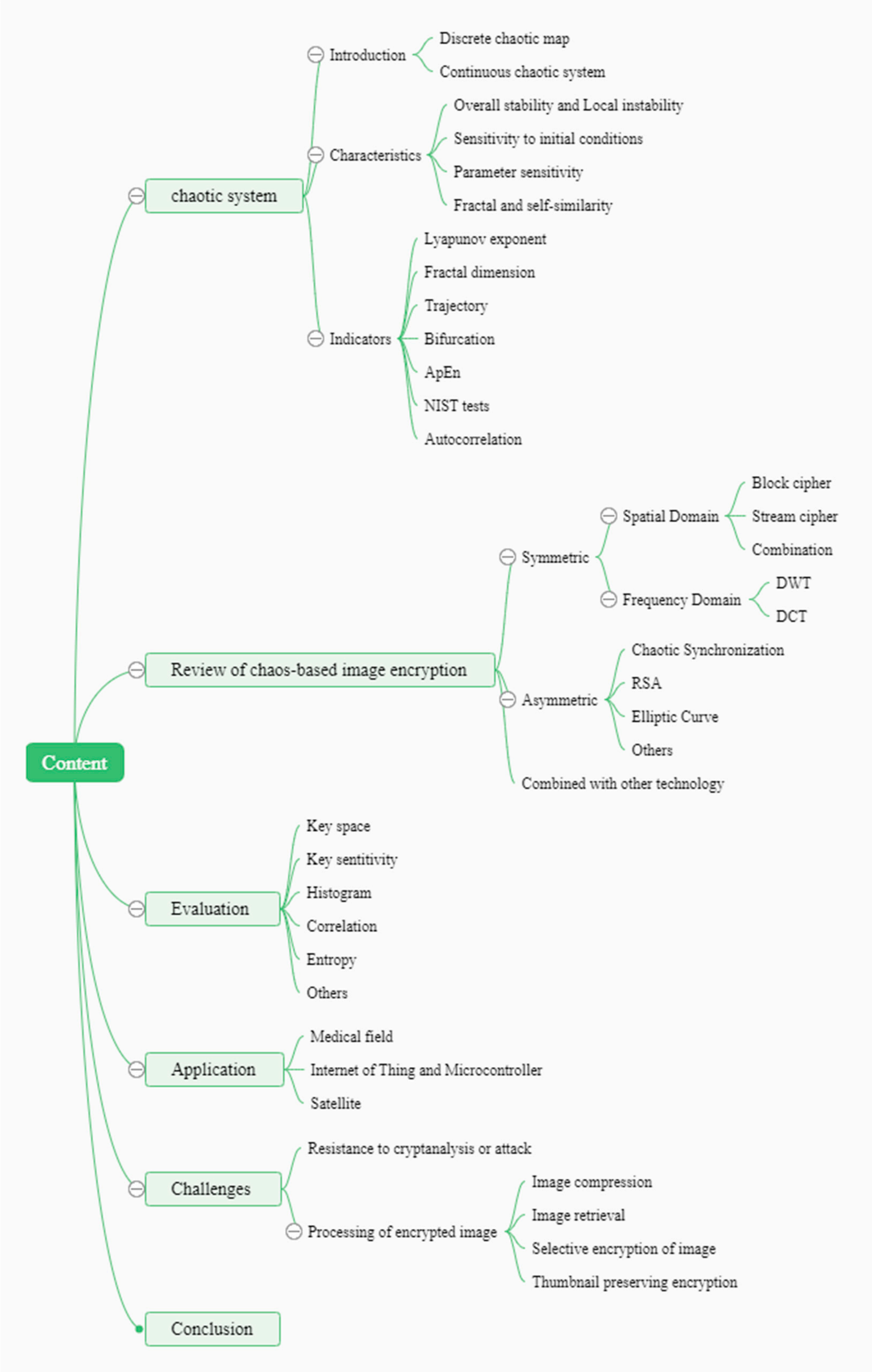

Figure 1. Content of the remaining sections.

2. Chaotic Systems

In this section, we first provide an introduction to chaotic systems, their characteristics, and some indicators to help readers better understand the following content.

2.1. A Brief Introduction to Chaotic Systems

Chaotic systems can be classified into two types based on the way they evolve over time: continuous chaotic systems and discrete chaotic maps [13]. A continuous chaotic system is one in which the state of the system evolves continuously with time, and its dynamical equations are typically a set of differential equations. Alternatively, a discrete chaotic map is a system whose state evolves discretely with time, and its dynamical equation is usually an iterative equation.

Discrete chaotic map: A discrete chaotic map is a dynamic system with discrete state variables that evolve over time. The discrete chaotic map is characterized by nonlinearity, sensitive dependence on initial conditions and parameters, and period multiplication, among other properties [14]. Several examples of discrete chaotic maps and their mathematical definitions are described below to provide a better understanding:

Logistic map [15]:

$$X_{t+1} = f_l\ (X_n) = p\ X_t\ (1 - X_t), \tag{1}$$

where $X_t \in (0, 1)$ is the state variable at time step t, $p \in [0, 4]$ is a control parameter, and $(1 - X_t)$ is the factor that limits the growth of the system. The Logistic map exhibits complex dynamical behavior when the parameter p is in the interval (3.57, 4].

Tent map [16]:

$$X_{t+1} = f_t(X_n) = \begin{cases} pX_t, & X_t < \frac{1}{2} \\ p(1 - X_t,), & \frac{1}{2} \leq X_t \end{cases}, \tag{2}$$

where $X_t \in (0, 1)$ is the state variable at time step t, $p \in [0, 2]$ is a control parameter, and the map is piecewise linear with a tent-shaped form.

Henon map [17]:

$$\begin{cases} X_{t+1} = 1 - aX_t^2 + Y_t \\ Y_{t+1} = bX_t \end{cases}, \tag{3}$$

where X_t and Y_t are the state variables at time step t, and a and b are control parameters. The Henon map is a nonlinear and dissipative system that exhibits complex dynamical behavior.

Arnold Cat map [18]:

$$\begin{cases} X_{t+1} = (2X_t + Y_t) \quad mod\ 1 \\ Y_{t+1} = (X_t + Y_t) \quad mod\ 1 \end{cases}, \tag{4}$$

where X_t and Y_t are the state variables at time step t. The Arnold Cat map is a chaotic system that exhibits complex dynamical behavior, including periodic, quasi-periodic, and chaotic regimes.

Discrete chaotic maps are suitable for applications such as digital signal processing and modulators in communication systems, and for image encryption and compression. The advantage of a discrete chaos map is that the mathematical model is relatively simple and easy to implement and compute; however, the disadvantage is that the parameter range is usually not large enough and the wrong selection of parameters can lead to rapid degradation of the dynamic characteristics of the system.

Continuous chaotic systems: Continuous chaotic systems are dynamic systems that exhibit complex and unpredictable behavior over time. These systems are usually described by a set of ordinary or partial differential equations that govern the evolution of state variables over time. The state variables represent physical quantities that are characteristic of the system under study, such as pressure, temperature, position, or velocity. Below we provide some examples of continuous chaotic systems and their mathematical definitions:

Lorenz equation [3]:

$$\begin{cases} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = \rho x - y - xz \\ \frac{dz}{dt} = xy - \beta z \end{cases}, \tag{5}$$

where x, y, and z are state variables, and σ, ρ, and β are control parameters named the Prandtl number, Rayleigh number, and direction ratio, respectively. The Lorenz equation is a nonlinear chaotic system that exhibits complex dynamic behavior. Its simple mathematical structure and rich dynamical behavior make it a popular model for studying the emergence of chaos in nonlinear systems. The Lorenz equation is characterized by having a chaotic attractor with a shape that resembles a butterfly, and it is particularly known for its sensitivity to initial conditions.

Chen system [19]:

$$\begin{cases} \frac{dx}{dt} = a(y-x) \\ \frac{dy}{dt} = (c-a)x - xz + cy \\ \frac{dz}{dt} = xy - bz \end{cases}, \tag{6}$$

where x, y, and z are state variables, and a, b, and c are control parameters. Moreover, the Chen system has a chaotic attractor and two unstable equilibrium points.

Rössler system [20]:

$$\begin{cases} \frac{dx}{dt} = -(y+z) \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = b + z(x-c) \end{cases}, \tag{7}$$

where x, y, and z are state variables, and a, b, and c are control parameters. The Rössler system typically shows spiral-like structures known as Rössler attractors in their state trajectories.

Continuous chaotic systems have the advantage of providing richer dynamical behavior and greater flexibility, but have the disadvantage of requiring higher computational power and more complex mathematical models, as well as the need for discretization to suit practical applications.

2.2. Typical Characteristics and Indicators of the Chaotic System

2.2.1. Characteristics

- Overall stability and local instability

Overall stability: The trajectory of a chaotic system will eventually be confined to a bounded region.

Local instability: The trajectories of the chaotic system separate at an exponential rate in some direction.

Overall stability and local instability are the most fundamental features of chaotic systems.

- Sensitivity to initial conditions

Chaotic systems are extremely sensitive to their initial conditions, which means that small changes in the initial state can lead to vastly different results. It shows the change in the overall performance of the system. This is the most distinctive feature of chaotic systems.

- Parameter Sensitivity

Small changes in the system to critical parameters can cause the system to exhibit completely different dynamical states. It shows the variation of the system's neighboring orbits.

- Fractal and self-similarity

The overall stability and the local instability make the chaotic system eventually form a self-similar hierarchy, i.e., a strange attractor. Strange attractors typically have a fractal structure, which means that they exhibit a consistent morphology at different scales. A strange attractor corresponds to a single trajectory. It is the long-term behavior of the system, assuming it is simulated for enough time. The strange attractors of chaotic systems usually exhibit fractal characteristics, i.e., they have similar structure and morphology at different scales.

2.2.2. Indicators

The chaotic dynamic characteristics of different chaotic systems are not identical, so some measures are needed to evaluate each chaotic system. Here, we introduce some relevant indicators to help readers understand this aspect.

- Lyapunov exponent (LE)

When two initial values with minimal error are applied to the same chaotic system, the trajectories they generate will be separated exponentially over time. *LE* is a tool used to visualize this phenomenon [21]. If we assume that $X_{n+1} = F\ (X_n)$ is a one-dimensional map, *LE* can be described as:

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum\nolimits_{i=0}^{n-1} \ln\left|F'(X_i)\right|. \tag{8}$$

When $LE < 0$, adjacent points tend to be stable, which means stable fixed points or periodic motion. When $LE > 0$, the orbital iterations with two different inputs diverge exponentially. LE can tell if the motion system is chaotic because the chaotic system has at least one positive LE, which is different from other stochastic systems. In addition, the larger the *LE* value, the more obvious the chaos characteristics. In addition, x-dimensional systems have x Lyapunov exponents. If a system has two or more positive Lyapunov exponents, it is called a hyperchaotic system.

- Fractal dimension

The main characteristic of the fractal is self-similarity, that is, there is some similarity between the part and the whole. The fractal dimension [+252] is an index used to describe the complexity of the system structure. Among the approaches used, the Box-counting method is the most widely used, and can be calculated by the following mathematical formula:

$$d = \lim_{r\to 0} \frac{\ln N(S,r)}{\ln(1/r)}, \tag{9}$$

where S is any nonempty bounded subset of an n-dimensional space, $N\ (S{,}r)$ is the smallest number of closed spheres of radius r used to cover S. The strange attractors of almost all chaotic systems have fractional dimensions.

- Trajectory

The trajectory diagram can directly show the ergodic property of a chaotic system and whether there is a cycle. For the one-dimensional discrete chaotic map, an ideal system should have a trajectory that exhibits no recognizable structure or periodic cycles, although trajectories of continuous chaotic systems often have some identifiable shape.

- Bifurcation

The bifurcation [22] diagram reflects the relationship between chaotic characteristics and control parameters. It enables the analysis of the variation in the system performance with parameters, and especially the sudden change in the system performance at the critical parameters. Figure 2 shows the Logistic map as an example of its period-doubling bifurcation.

- Approximate entropy (ApEn)

ApEn [23] is one of the metrics used to measure the complexity of time series. For time series, the larger the value of ApEn, the higher the orbital complexity generated by chaos.

- NIST Statistical Tests

The NIST Statistical Suite [24] uses 16 separate statistical verification tests when verifying the randomness of binary sequences. In the NIST statistical tests, the significance level is set at 0.01. When the p-value of the sequence to be tested is $\geq$0.01, the sequence is considered to pass the statistical test. Currently NIST statistical tests are considered the current criteria for random testing.

- Autocorrelation

Autocorrelation describes the degree of correlation between the states of a random process itself at any two different times. The autocorrelation of an ideal chaotic sequence should decay rapidly with the interval of states.

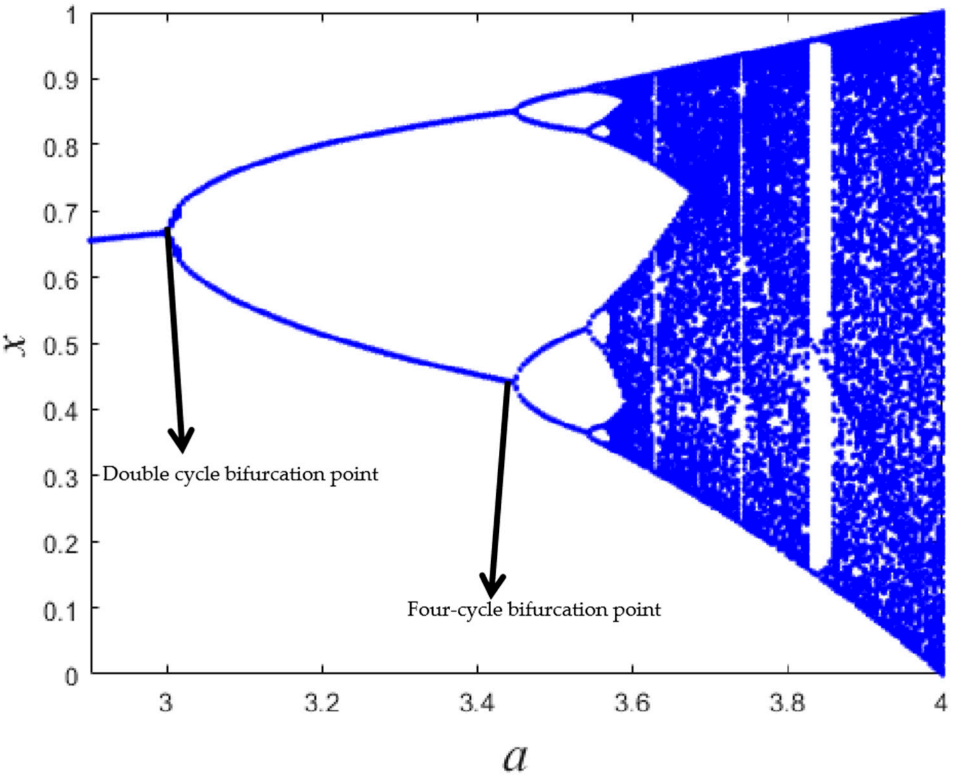

Figure 2. Period-doubling bifurcation of the Logistic map.

3. A Review of Chaos-Based Image Encryption

Chaos-based image-encryption technology can be categorized into different types based on various classification methods. One approach is to classify it according to how the original image is processed, which can be divided into chaotic image encryption based on a block cipher and chaotic image encryption based on a stream cipher. Additionally, it can be categorized based on the characteristics of the key, which can be divided into symmetric key chaotic image encryption and asymmetric key chaotic image encryption. In this section, we introduce chaos-based image encryption based on these two classifications.

It is worth noting that the schemes introduced in the following sections are discussed by default in the order of their publication year. Additionally, it is assumed that readers have some basic understanding of chaotic systems.

3.1. Chaos-Based Image Encryption Based on Symmetric Encryption

In symmetric encryption, encryption and decryption require a single key known as the private key or secret key. The encryptor and decryptor both use this same key, and a secure channel is needed to transmit the key. When applied to image encryption, symmetric encryption can be divided into spatial-domain chaotic image encryption and frequency-domain chaotic image encryption based on the transform domain used for encryption.

3.1.1. Chaotic Image Encryption Based on the Spatial Domain

In image encryption, the term spatial domain refers to the image itself. Since digital images are composed of a large number of pixels, spatial-domain-based image encryption means directly operating on these pixels. This can include shuffling image pixels or blocks, changing the value or position of pixels in the original image, and other similar operations.

At present, most chaotic image-encryption algorithms employ spatial-domain encryption, while others use frequency-domain encryption, as discussed in Section 3.1.2.

The main structure of a spatial-domain-based chaotic image-encryption algorithm is based on a permutation–diffusion architecture, which consists of two phases of iteration. In the permutation phase, the position of the image pixel is changed while retaining the original value. In the diffusion phase, the pixel values are sequentially modified, so that even a small change in the pixel will influence almost all the pixels in the entire image. The process is illustrated in Figure 3.

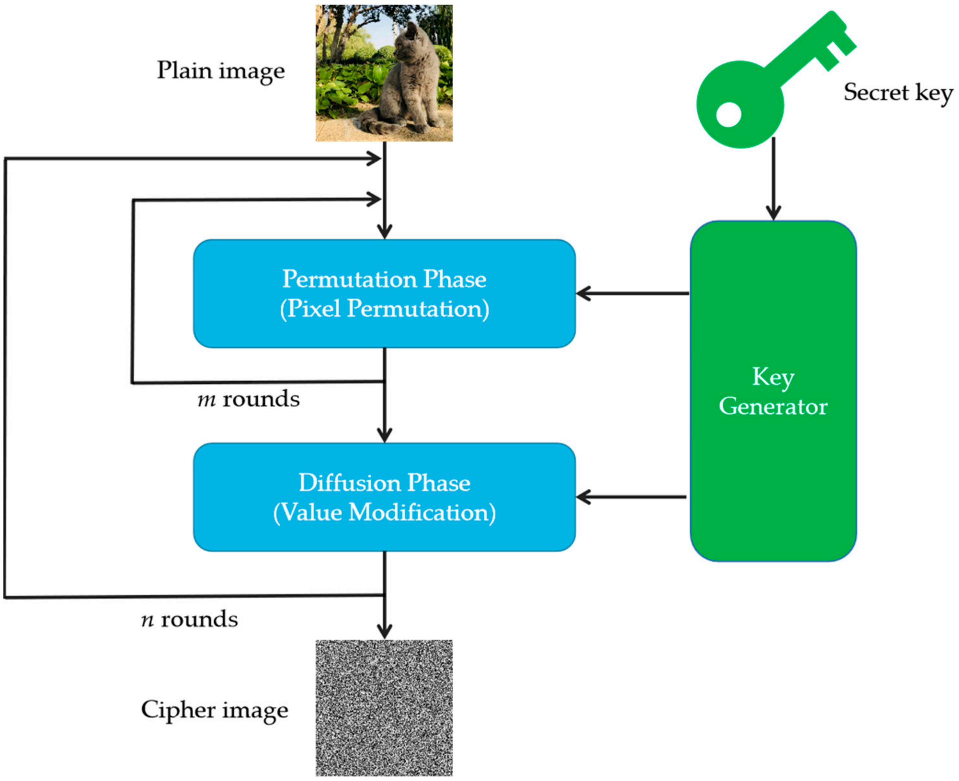

Figure 3. The architecture of permutation–diffusion chaotic image encryption.

Symmetric spatial-domain image-encryption algorithms can be divided into two types based on the way the original image is processed: block cipher and stream cipher. In block-cipher-based image-encryption algorithms, the image is encrypted or processed in fixed-length groups of bits called blocks. In stream-cipher-based image-encryption algorithms, the digital image is converted into streams of bits for processing [11].

Chaotic Image Encryption Based on the Block Cipher

A block cipher is a type of symmetric key algorithm that divides the plaintext into multiple blocks of equal length, and then encrypts each block separately using a specific algorithm and key. There are five modes of block cipher: ECB, CBC, CFB, OFB, and CTR. The idea of chaotic image encryption based on a block cipher is to use a chaotic map to generate secret keys or chaotic sequences to substitute and diffuse the pixels or bits of the image to achieve a higher level of security.

F. Pichler and J. Scharinger [25] first proposed an encryption scheme based on a two-dimensional Baker map. After that, in 1996, Jiri Fridrich [25,26] introduced a five-step process for building block ciphers: designing the basic map, generalizing the map, discretizing, extension to three dimensions, and composing with a diffusion mechanism. In addition, an encryption algorithm that adapted certain invertible chaotic two-dimensional maps to create new symmetric block encryption schemes was proposed, in which the chaotic map could be further extended to three dimensions. This scheme is effective in encrypting a large amount of data, such as that of a digital image.

Instead of the usual operation on small data blocks, a scheme involving parametrizable permutations on large data blocks (whole images) induced by Kolmogorov flows was presented by Josef Scharinger [27]. He emphasized the importance of confusion and diffusion, took the whole image as a single block, and applied a pseudo-random number generator (PRNG) based on Kolmogorov flows to confuse data. PRNG was widely used in subsequent chaotic image-encryption algorithms. Kolmogorov flows are a stochastic model of flow in which the velocity field is highly irregular and complex, manifesting itself in phenomena such as vortices and turbulence. Furthermore, the velocity field of Kolmogorov flows also has the characteristic of being the same in any direction. Here, we briefly describe the discrete model of Kolmogorov flow as follows:

$$T_{n,\delta}(x, y) = (q_s(x - F_s) + (y \bmod q_s), F_s + (y \operatorname{div} q_s)) \tag{10}$$

where $\delta = (n_1, n_2, \ldots, n_k)$, n_s is a positive integer, $\sum_s n_s = N$ and n_s divides N for all s, $p_s = 1/n_s$, and F_s is still the left bound of the vertical strip s.

The above schemes have inspired a large amount of subsequent research on chaotic image encryption. We classify block-cipher-based chaotic image encryption in terms of various perspectives, as follows:

- Algorithms when chaotic systems are employed as the PRNG

The PRNG is the most common application of chaotic systems when applied in encryption algorithms [28,29]. A PRNG is used to generate chaotic sequences for operations such as XOR, confusion, and diffusion. Many characteristics of chaotic systems coincide with those of traditional cryptography. For example, the orbital instability and initial value sensitivity correspond to the diffusion characteristics of traditional cryptography systems, while the ergodic and long-term unpredictability of chaotic systems, and sensitivity to system parameters, correspond to the chaotic characteristics of traditional cryptography. It can be seen that using chaotic systems as a PRNG to generate pseudo-random sequences has certain advantages.

Masaki Miyamoto and Kiyoshi Tanaka [30] proposed a new truncated Baker transformation with finite precision. In this scheme, a random local rotation operator is incorporated between two neighbor elements in the mapping domain in order to keep the same precision.

J. Yen and J. Guo [31] presented a chaotic image-encryption algorithm that substitutes all blocks of the original image and then shuffles its pixels with a chaotic sequence generated by a Logistic map based on the permutation principle. Its VLSI architecture is also presented in their paper.

In contrast to previous chaos-based image-encryption algorithms [31,32], which required the image to be encrypted as a square, in 2003 Mazleena Salleh [33] proposed an alternative chaotic image-encryption method based on a Baker map. The enhanced symmetric algorithm can support the encryption of images with a variable size. In addition, this scheme adds some other features such as password binding, ECB, and CBC modes to make the cipher image more secure.

Shiguo Lian and Jinsheng Sun [34] proposed a chaos-based image-encryption method that utilizes a 2D Standard map for confusion, a Logistic map for diffusion, and a Tent map to generate keys for sub-key generation and distribution because of its multiple processes. Then, a certain diffusion effect in the substitution stage caused by simple sequential add-and-shift operations was added to the scheme in [35] to save a considerable amount of overall encryption time.

Zhihong Guan [36] suggested a 3D Chen's chaotic-system-based image-encryption method. The three discrete variables sequences obtained by Chen's system after iteration and preprocessing were XOR with different sub-blocks of the original image to obtain the encrypted image. Di Xiao and Xiaofeng Liao [37] analyzed the flaws of the image encryption proposed in [36] and improved it in terms of three aspects: the phase of encryption or decryption needs M rounds of operations; the keystream depends on both the initial conditions and the plain-image gray value; the keystream is generated by chained mode, with any two adjacent pixels being linked to each other. This makes the chaining relation between pixel elements more complex after M rounds of iteration.

A Logistic-map-based image encryption was introduced by Tao Xiang and Xiaofeng Liao [29] on the basis of [38], in which the plaintext block is permuted by a key-dependent shift approach and then encrypted by the permutation–diffusion-based technique.

N. K. Pareek and V. Patidar [39] proposed an approach for image encryption based on Logistic maps. They used two Logistic maps in the algorithm. The first one is used to generate numbers ranging from 1 to 24 as the initial condition of the second Logistic map. Furthermore, an external 80-bit secret key and eight different types of operations are used to encrypt the pixels of an image, and which of these is used for a particular pixel is decided by the outcome of the Logistic map.

An image-encryption method based on primitive operations, nonlinear transformation functions, and a chaotic Tent map was presented by Mohamed Amin and Osama S. Faragallah [16]. The cryptographic operation of this algorithm is based on bit blocks rather than pixel blocks. It uses 256-bit session keys to encrypt a 256-bit input plain image into the cipher image with the same number of bits.

Y. Wang and K. Wong [40] introduced the nearest-neighbor coupled-map lattices (NCMLs), in which a pseudo-random sequence is generated with an NCML and an S-Box of AES. In addition, a 128-bit external key is used to reset the pixel values of the image blocks with the pseudo-random sequence. Meanwhile, the lattice values of the NCML are utilized to relocate image blocks.

J. S. Armand Eyebe Fouda and J. Yves Effa [41] proposed a PWLCM-based chaotic image-encryption method that uses the Linear Diophantine Equation (LDE). The LDE is an equation with integral coefficients of one or more variables, for which the solutions must be integers.

A new 1D chaotic system based on a Logistic map was introduced by Erivelton G. Nepomuceno and Lucas G. Nardo [42], which was then employed in image encryption to reduce the digital degradation of chaotic systems with key space. The pseudo-random sequence was generated by the difference between two pseudo-orbits for image encryption.

- Chaotic image-encryption algorithms with improved performance or chaotification

However, classical chaotic systems have some inherent limitations, such as periodicity, small key space, easy destruction of phase space, and low LE. To address these issues, many researchers have focused on improving classical chaotic systems to enhance their chaotic dynamic characteristics through a process called chaotification. The goal of chaotification is to make up for these limitations and improve the performance of chaotic systems in applications such as encryption algorithms.

Guanrong Chen and Yaobin Mao [18] introduced a real-time secure symmetric encryption model by extending a two-dimensional chaotic Cat map to three dimensions to quickly eliminate the correlation between pixels. Before confusion and diffusion, the original image was expanded from 2D to 3D by the following representation. The original image, which is L pixels wide and H pixels high, is divided into several cubes with side lengths of $\mathrm{N_i}$, and satisfies the following conditions:

$$L \times H = \Sigma\, {N_i}^3 + R, \tag{11}$$

where $N_i \in \{2, 3, \ldots, M\}$, M is the maximum side length of the cube, and $R \in \{0, 1, \ldots, 7\}$ is the remainder. On this basis, each cube was shuffled and XOR diffused using a discrete 3D Cat map and Logistic mapping, respectively. Finally, all the cubes were properly arranged and returned to two dimensions to obtain the encrypted image. The specific process is shown in Figure 4.

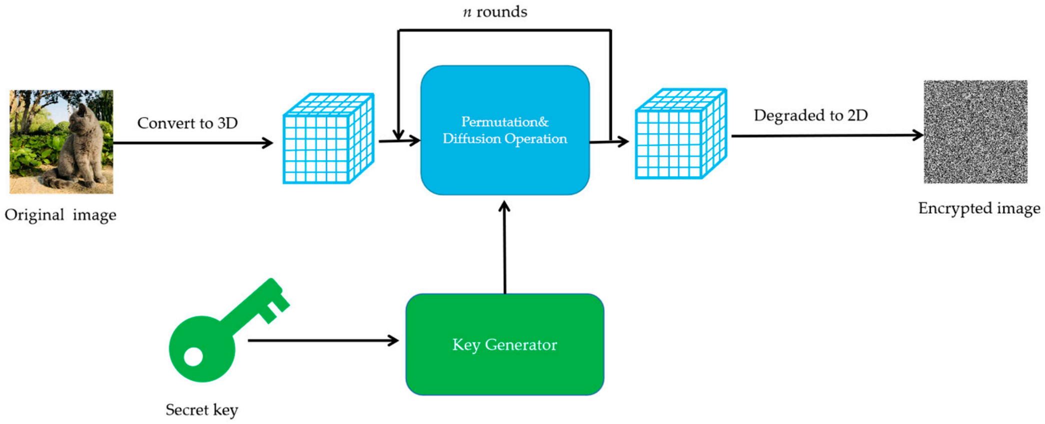

Figure 4. The process of the image-encryption algorithm in Ref. [18].

Yaobin Mao and Guangrong Chen [38], based on the achievement of F. Pichler and J. Scharingers [43], further extended a two-dimensional Baker map to three dimensions with better chaotic characteristics in LE for fast image encryption while retaining its high security. In contrast to Ref. [18], the original image was preprocessed into a whole cube of size M × N × L before being encrypted. This algorithm has a significant advantage in terms of speed.

An image-encryption scheme based on a chaos-based map with variable control parameters was presented by Yong Wang and Kowk-Wo Wong [44]. The 2D Standard map, the Cat map, and the Baker map were employed in the permutation stage, but which of these is used is decided by the Logistic map. The outstanding contribution is that control parameters and the keystream are related to both the key and the plain image.

Xiaojun Tong and Minggen Cui [45] proposed a compound two-dimensional chaotic map to generate a chaotic sequence for dividing an image by employing two one-dimensional chaotic maps that switch randomly. Then, the image is encrypted by a 3D Baker map. They solved the problem of computer-limited precision owing to the low-digitalized one-dimensional chaotic function using dynamical compound chaos and perturbation technology.

Xiaoling Huang [46] added parameters to a two-dimensional cross-chaotic Chebyshev system. Then, the new function, which has a large key space and is sensitive enough to initial conditions, was employed to generate a pseudo-random chaotic sequence for confusion and diffusion.

Guodong Ye and Kwok-Wo Wong [47] proposed an image-encryption algorithm with a generalized Arnold Cat map. They utilized a total circular function to take the place of the traditional periodic position permutation to reduce the correlation between adjacent pixels in the permutation stage. Two pseudo-random sequences generated by a Cat map with different initial conditions were utilized in forward and reverse diffusion.

The traditional permutation process is periodic, which enables an attacker to obtain the original image by iterating over the encrypted image. Furthermore, it is also weak against chosen-plaintext attacks. Xingyuan Wang and Lintao Liu [48] introduced a dynamic random growth technique in their Cat-map-based image-encryption method to fill those two gaps.

Jun-xin Chen and Zhi-liang Zhu [49] proposed a dynamic state variables selection mechanism (DSVSM)-based image-encryption algorithm. They used a Chen map to illustrate DSVSM and innovated the algorithm in four ways to fix its flaws.

Lingfeng Liu and Suoxia Miao [50] presented a Logistic-map-based image-encryption method with varying parameters. Their approach can make the parameters change in a random way to improve robustness to the phase space reconstruction attack.

In Chanil Pak and Lilian Huang's article [51], two of the three 1D chaotic maps (Logistic map, Sine map, and Chebyshev map) were used to construct a new chaotic system, which has both high information entropy and a Lyapunov exponent, for encryption. The linear (permutation)–nonlinear (diffusion) structure-based chaotic image encryption is improved to a linear–nonlinear–linear conversion structure-based algorithm.

The limited accuracy of computers results in the degradation of the chaotic characteristics of a chaotic system. Lucas G. Nardoa and Erivelton G [52] took finite accuracy error as the source of randomness and proposed a new image-encryption scheme to solve this problem. The Chua system and a factor based on the plain image were used together to generate the keystream, which was then used in conjunction with the XOR operation to encrypt the image.

It is well-known that a chaotic system with a useful large LE implies the properties of excellent chaos. However, an image-encryption scheme based on chaotic systems with a small LE was proposed in [53]. The authors utilized a chaotic system with a low numerical solution error to reduce the decryption error and proved its positive effect by conducting experiments on an XOR encryption scheme. This strategy is suitable for the Lyapunov exponent control method of an arbitrary chaotic interval map.

Hua and Z. Zhu [54] constructed a 2D Logistic-Tent modular map called 2D-LTMM to overcome shortcomings. Then, a color image-encryption algorithm, which utilized cross-plane permutation and non-sequential diffusion to concurrently encrypt the three color planes of images, was presented based on 2D-LTMM.

- Block-cipher-based image encryption with a coupling chaotic system

A coupled system can be regarded as a high-dimensional dynamical system formed by the interaction of two or more chaotic maps. Thus, coupling chaotic systems are also often constructed by researchers for image encryption because of their special advantages: high complexity of the output cipher image and effective byte confusion and diffusion, in addition to a conventional chaotic map. All these features are useful for high security of the image-encryption algorithm.

S. Behnia and A. Akhshani [55] were the first to mix the Logistic map with a coupled map based on [56,57] for image encryption. This mixture scheme has large key space and high-level security, although its speed is only acceptable.

Seyed Mohammad Seyedzadeh and Sattar Mirzakuchaki [58] also introduced an image cryptosystem based on their Two-Dimensional Piecewise Nonlinear Chaotic Map (CTONCM).

Yicong Zhou and Long Bao [59] designed a new chaotic system by coupling two of the Logistic map, Tent map, and Sine map as a new chaotic map for image encryption. Their scheme has some useful properties; in particular, it will generate a brand-new encrypted image each time it is used with the same set of security keys for an original image.

In Moatsum Alawida and Azman Samsudin's image-encryption algorithm [60], three 1D chaotic maps (Tent map, Logistic map, and Sine map) are employed as a seed map to couple into new chaotic systems, the Tent–Logistic–Tent system (TLTS) and Tent–Sine–Tent system (TSTS). Both of these two new chaotic systems are used for permutation and diffusion processes.

- Block-cipher-based image encryption with a hyperchaos system

Due to the finite accuracy of computers, the period of chaotic systems with low dimensions may be shorter in practical use, and their key space may be relatively small. Therefore, some researchers suggest using hyperchaotic systems with more than one positive LE for image encryption to generate higher complexity and randomness.

Tiegang Gao and Zengqiang Chen [61,62] were the first to employ hyperchaos systems as a PRNG for diffusion of image encryption. A total matrix generated by a Logistic map was utilized to shuffle the position of image pixels. After that, a hyperchaotic system or a combination of the Lorenz equation and Chen map was presented to confuse the relationship between the plain image and cipher image. However, their algorithm is not safe enough because the keystream in the diffusion phase only depends on the state variables of the hyperchaotic system.

Congxu Zhu [63] presented an improved hyperchaos-based image-encryption method, in which the keys are correlated with the plain image. In addition, it only takes two rounds of diffusion operation to modify values of the pixel and break the correlation between adjacent pixels of the image.

Hegui Zhu and Cheng Zhao [64] proposed a compression-based image-encryption method with a combination of a hyperchaos system and the Chinese remainder theorem. Two chaotic sequences are generated by a 2D hyperchaos discrete nonlinear system to shuffle the pixels of the plain image, and the Chinese remainder theorem is used for encryption and compression.

Wenhao Liu and Kehui Sun [65] drew on the characteristics of [61] to introduce a hyperchaos-based image-encryption method with a two-dimensional Sine iterative chaotic map with infinite collapse (ICMIC) modulation map (2D-SIMM) based on a close-loop modulation coupling (CMC) model. They noted that chaotic shift transform (CST) is efficient for permutation.

Fei Yu and Si Xu [66] introduced an image-encryption scheme based on a 5D memristive exponential hyperchaotic system (MEHS). To construct this system, they utilized flux-controlled memristors and added a nonlinear exponential term, resulting in a new memory hyperchaotic system. Additionally, a hardware circuit for this system was designed using Field Programmable Gate Array (FPGA) technology. The algorithm was thoroughly tested for security, and the results indicated that it is sufficiently robust.

- Algorithms when chaotic systems are combined with S-Boxes

Combining chaotic systems with traditional cryptographic methods, such as substitution boxes (S-Boxes), can effectively defend against attacks and enhance the security of cryptographic systems. This combination can take advantage of the strengths of both chaotic and traditional cryptographic techniques, creating a more robust encryption algorithm that is resistant to attacks and can ensure the confidentiality and integrity of the encrypted image.

In Linhua Zhang and Xiaofeng Liao's AES-based algorithm [67], the S-Box is designed with a discrete exponential chaotic map (DECM) and the chaotic sequence is generated by a 1D Piecewise Linear Chaotic Map (PWLCM) to perform permutation and XOR diffusion operations.

Alireza Jolfaei and Abdolrasoul Mirghadri [68] constructed an image-encryption scheme with a Baker map and a Simplified AES (S-AES) algorithm. The Baker map is used to generate dynamic S-Boxes to take the place of the S-Box of S-AES.

Afterward, a parallel chaos-based image-encryption method, called MASK, was proposed by Qing Zhou and Kwok-wo Wong [69] based on discretized Kolmogorov flow and traditional CBC-like mode. The S-Box generated by a Chebyshev map is used for S-transformation and the Kolmogorov flow is used for K-transformation.

- Chaotic image-encryption algorithms based on bitplane operation

Most of the proposed image-encryption algorithms typically move each pixel separately from one position to another without modifying its value, which may limit the effectiveness of the encryption. However, some encryption methods decompose the image into bitplanes and operate on each bitplane separately, which can make up for these deficiencies. By operating on each bitplane independently, the encryption algorithm can achieve a higher level of security and improve the efficiency of the encryption process.

Guosheng Gu and Guoqiang Han [70] added a cross-sampling method to 1D chaotic image encryption to eliminate the recursive relations between the binary chaotic pseudorandom sequences. A discrete chaotic map was used to generate an ergodic matrix to arrange the positions of bits. Then two binary chaotic random sequences are generated to replace the corresponding values.

Zhiliang Zhu and Wei Zhang [71] presented an image-encryption method whose operations of permutation and diffusion are at the bit level. The 2D Arnold Cat map controlled by the Logistic map was employed to construct a permutation matrix for confusion, and the value of each pixel was modified by the output of the Logistic map.

In Xinsheng Li and Zhilong Xie's 7D hyperchaotic-system-based image-encryption approach [72], the 2D image at the pixel level was converted into a 3D cuboid in a bitplane for some operations such as rearranging, symmetry, rotation, zigzag, and global bit permutation, with the pseudo-random sequence generated by the new chaotic system.

A bitplane matrix rotation-based image-encryption algorithm with two hyperchaotic systems was proposed by Cong Xu and Jingru Sun [73]. The original image is first decomposed into 8-bit planes, which are further formed as a 3D bitplane matrix of size M × N × 8. Then, a PRNG generated by a hyperchaotic system is used to control the rotation of the submatrix of the 3D bitplane matrix in different directions. Finally, the pixel value of the intermediate image is modified using another keystream.

In order to reduce the shortcomings of high complexity and the many operation processes of many encryption algorithms, Jiangjian Xu and Bing Zhao [74] introduced a color image-encryption algorithm based on bitplane information. They converted each pixel value to two hexadecimal numbers for low complexity. The initial parameters of the chaotic system used in the encryption process of each channel in the color image are related to the plaintext information of the current channel and the other two channels, which made the key space larger.

Wei Song and Chong Fu [75] proposed a parallel image-encryption algorithm based on intra-bitplane scrambling. Their contribution was to use four threads for bit-level image encryption, where each thread scrambled two bitplanes during the permutation process and built multiple threads to generate the keystream to reduce encryption time during diffusion.

- Color chaotic image-encryption algorithms based on the block cipher

Many encryption algorithms have been proposed for grayscale images, but the encryption of color images, which are divided into red (R), green (G), and blue (B) channels, needs improvement in some aspects due to the high correlation between the R, G, and B components. It is also worth investigating how to handle these three channels during the encryption process to ensure the confidentiality and integrity of the encrypted data. Further research is needed to develop effective encryption algorithms for color images that can address the limitations of current approaches and provide a higher level of security.

Vinod Patidar and N. K. Pareek [76] presented a lossless symmetric image-encryption algorithm based on the same architecture, which is helpful for encrypting the colored image, whose data stream is a 3D matrix, with a 2D Standard map and a 1D Logistic map. In this scheme, the red, green, and blue channels of the original image are extracted for the XOR confusion and diffusion operation with the chaotic sequence generated by the Standard map.

C. Huang and H. Nien [77] used these four chaotic maps for color image encryption: the Henon map, Lorenz equation, and Chua and Rössler systems. In their algorithm, the distribution characteristics of RGB were effectively disrupted and the robustness to exhaustive attacks was improved at the same time.

A color image-encryption algorithm based on a three-dimensional Arnold Cat map was proposed by A. Kanso and M. Ghebleh [78]. The algorithm can be valid for color images of any size. The encryption process contains three steps: shuffling the image pixels according to a search rule based on the 3D Cat map in step 1; and using 3D Cat maps to shuffle pixels through mixing and masking rules in steps 2 and 3, respectively. These rules make the relationship between the plain image and the encrypted image more diffusing and confusing.

Wang Ying [79] applied a high-dimensional Lorenz equation to digital image encryption, whose 3D outputs can realize the parallel encryption of three or more images. Therefore, it is suitable for layered encryption of three-dimensional data such as color images.

Zhihua Gan and Xiuli Chai [80] proposed a 3D bitplane permutation-based image-encryption method. A new method for generating a secret key matrix was presented. The Chen system was used to generate random sequences to perform confusion and diffusion operations multiple times on small 24-bit blocks consisting of three 8-bit blocks from the R, G, and B channels of the original image. Their approach is effective against the known-plaintext attack and chosen-plaintext attack.

Chaos-Based Image Encryption Based on Stream Cipher

Stream ciphers are widely used in cryptographic fields due to their fast operation speed and high security performance. The keystream generator plays a critical role in the stream cipher, as its performance directly determines the security performance of the algorithm. Therefore, the combination of chaotic systems and stream ciphers relies heavily on the integration of chaotic maps and keystream generators. Currently, the primary method of applying chaos to a stream cipher is by constructing keystream generators using chaotic systems [48].

- Stream-cipher-based image encryption with the classic chaotic system

Haojiang Gao and Yisheng Zhang [81] improved the original Logistic mapping by transforming it into a nonlinear chaos algorithm (NCA) by introducing a power function and a tangent function. Then they applied it to a one-time-one-password system for image encryption.

A Chaotic Key-Based Algorithm (CKBA) and its Very Large Scale Integrated Circuit (VLSI) architecture based on any 1D chaotic system were recommended by Jui-Cheng Yen and Jiun-In Guo [82] in their article. They produced a sequence as the key with a chaotic map, then the pixels of the image were rearranged and XOR or XNOR operated with the selected key. However, Shujun Li and Xuan Zheng [83] estimated its security and pointed out that this algorithm is weak for the known-plaintext attack, which implies that the security of the algorithm needs to be improved.

In 2007, H. S. Kwok and Wallace K. S. Tang [84] suggested a fast chaos-based image-encryption system with a stream-cipher structure, where the PRNG is formed by a 1D Tent map and a H-D Cat map, serving the purpose of stream generation and random mixing. Unlike the other existing chaos-based pseudo-random number generators, this type of keystream generator has very fast throughput under finite precision representation and fixed-point arithmetic.

Liu Hongjun and Wang Xingyuan [85] designed a one-time key encryption system based on two robust chaotic maps to solve some problems of previous chaos-based image-encryption systems. The true random number generator (TRNG) was utilized to generate the keys by the Message-Digest algorithm 5 of the mouse positions.

- Stream-cipher-based image encryption with the coupled chaotic system

As mentioned above, a large number of classic chaotic systems have been applied to stream-cipher-based image encryption. Although they have high efficiency and fast speed, these chaotic maps have some disadvantages, such as weak security and small key space. Therefore, the coupling of low-dimensional chaotic maps may show a new way for stream-cipher-based image encryption.

A symmetric streaming chaos-based image-encryption algorithm which was designed for encrypting color images was proposed by Sahar Mazloom and Amir Masud Eftekhari-Moghadam [86] based on their coupled nonlinear chaotic map (CNCM). Shubo Liu and Jing Sun [87] introduced a coupled Logistic map as a keystream generator. Their stream-cipher-based image-encryption scheme with this key generator illustrates that it can be a good substitute for the block cipher.

Inspired by TRNG, an idea for a chaos-based true random bits generator (TRBG) with the interaction between two mutually coupled identical chaotic circuits was introduced by Ch. K. Volos and I. M. Kyprianidis [88]. Then, a new chaos-based image-encryption approach was presented.

- Stream-cipher-based image encryption with the spatiotemporal chaotic system

The spatiotemporal chaotic system, which is confirmed to have a longer periodicity and has nonlinear dynamics in both space and time, is very suitable for cryptography and image encryption. The spatiotemporal chaotic system not only has chaotic behavior in time, but also in space after a long time iteration. The most classic approach is the coupled-map lattice (CML), which is described as follows:

$$x_{n+1}(i) = (1-\varepsilon)f[x_n(i)] + \frac{\varepsilon}{2}\{f[x_n(i+1)] + f[x_n(i-1)]\}, \tag{12}$$

where x_n (i) represents the state variable of the ith site (i = 1, 2, . . . , $S \in N$, S is the number of the sites in the CML) at time n (n = 1, 2, . . .), ε is the coupling parameter, f (x) is the Logistic map.

Because of the intrinsic nonlinear dynamics of each local map and the diffusion due to the spatial coupling among the local maps, a CML exhibits spatiotemporal chaos [89]. It consists of nonlinear maps called local maps on the lattice sites. Each local map is coupled with other local maps governed by certain coupling rules.

A. N. Pisarchik [90] was the first to apply CML to an image-encryption algorithm, whose basic idea is to convert the image color under initial conditions into the Logical map pixel by pixel.

The one-way coupled-map lattice (OCML), as an example of a spatiotemporal chaotic system, was often applied to symmetric stream-cipher-based image encryption [91,92]. Rhouma Rhouma and Soumaya Meherzi [87] selected a 192-bit external key to generate the parameters and the initial conditions of the OCML.

Fuyan Sun and Shutang Liu [93] proposed 2D CML-based chaotic image encryption, which takes only one operation cycle and renders the image indistinguishable.

Different from the above schemes, an image-encryption method based on mixed linear–nonlinear coupled map lattices was proposed by Zhang Ying-Qian and Wang Xing-Yuan [94]. The algorithm with this kind of spatiotemporal system has less periodic windows and a larger range of parameters.

In Zhang Ying-Qian and Wang Xing-Yuan's algorithm [95], the non-adjacent coupled map lattice (NACML),which has a wider range of parameters and fewer periodic windows in the bifurcation diagram than 1D chaotic systems, is selected in the diffusion process. Furthermore, a new bit-level permutation method is used to effectively reduce the intrinsic features and spatial complexity of the algorithm.

Chaos-Based Image Encryption Based on Both Block and Stream Ciphers

In addition to applying the block cipher or stream cipher to image-encryption algorithms, some researchers have attempted to combine these two strategies in image encryption, which aims to enhance the robustness of the algorithm and increase its implementation efficiency.

Fethi Belkhouche and Uvais Qidwai [96] presented an algorithm for binary images using chaotic mapping based on a modified version of a sine function. The algorithm can quickly encrypt binary images in real time.

An image-encryption method using two chaotic maps and combining the spatial-domain encryption and stream ciphers was introduced by Huangpei Xiao and Guoji Zhang [97]. They used chaotic maps to generate the chaotic sequence for modifying the pixel values of the plain image and to construct a permutation matrix for encrypting the modified image.

Xingyuan Wang and Xiaojuan Wang [98] proposed a scheme that uses a block cipher and a stream cipher alternately for image encryption. They utilized PWLCM and two other 1D chaotic maps to generate pseudo-random sequences to decide the encryption mode. In Hongjun Liu and Xingyuan Wang's approach [99], PWLCM, as the substitution of a Cat map, is first used to rearrange the image at the bit level. After that, the three discrete variables of the Chen map are used to encrypt the image again for confusion and diffusion. A new bit-level image-encryption method with PWLCM and binary bitplane decomposition (BBD) was proposed by Lu Xu and Zhi Li [100]. The BBD is used before permutation and diffusion to switch the plain image to two binary sequences while the PWLCM is employed in the diffusion phase to control the swapping of the binary elements of these two sequences.

Different from the conventional permutation–diffusion-structure-based scheme, Yuling Luo and Minghui Du [101] suggested an image-encryption algorithm with the reverse process, which first diffuses with a nonlinear spatiotemporal chaotic map and integer wavelet transform (IWT), and is later rearranged with a Logistic map.

3.1.2. Chaos-Based Image Encryption Based on the Frequency Domain

The advantages of spatial domain algorithms are their fast computation speed and the fact that the encryption process does not cause additional image distortion. However, the robustness of the spatial-domain encryption may not be satisfactory. In contrast, frequency-domain encryption algorithms offer high efficiency, and the complexity of their mathematical expressions makes it more difficult to illegally decode the encrypted image. Therefore, many researchers choose to combine frequency-domain encryption with chaotic encryption to construct new image-encryption algorithms. It should be noted that the original image needs to be preprocessed, as shown in Figure 5, before using such methods to encrypt it.

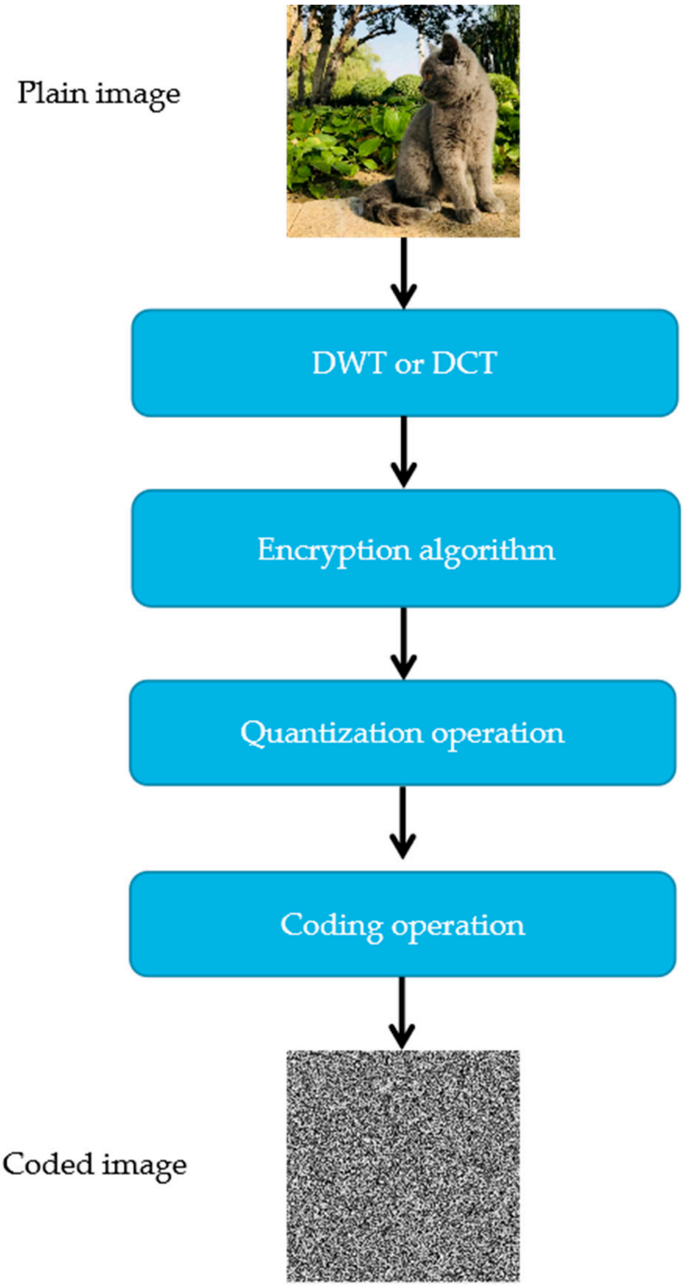

Figure 5. The process of frequency-domain-based image encryption.

- Discrete Wavelet Transform (DWT)-based algorithms

DWT can divide signals with both frequency and time information into different sub-bands, which can result in a higher compression ratio and better rendering of the image by eliminating blocky artifacts. DWT is a powerful tool for image processing and has been widely used in image compression, denoising, and feature extraction. By decomposing the image into different frequency sub-bands, DWT-based encryption algorithms can achieve a higher level of security and provide better protection against attacks.

Chun-jiang Pang [102] first presented a DWT-based image encryption with a 2D Cat map in 2009. An exclusive corresponding relationship between the Cat map chaos sequence and the DWT coefficient matrix is established according to the value sequence generated by the Cat map. Afterwards, the DWT matrix is encrypted, and then scrambled by a chaotic sequence.

Somaya Al-Maadeed and Afnan Al-Ali [103] introduced a technique with the combination of encryption and compression. They used DWT to decompose the image and decorrelate its pixels into the main (low-frequency) part and the detail (high-frequency) part. The main part contains the overall shape and contour of the image, while the detail part only contains fine details. The approximation component is encrypted by a 1D discrete chaotic map, and the detail components are compressed by DWT.

Xiangjun Wu and Dawei Wang [104] combined the frequency-domain cryptosystem and the spatial-domain cryptosystem and proposed a lossless image-encryption algorithm, which makes full use of the advantages of image encryption in the spatial domain and the transform domain, based on 2D DWT and a 6D hyperchaos-based system.

- Discrete Cosine Transform (DCT)-based algorithms

A 2D Cat-map-based image-encryption scheme with DCT was proposed by Zhengjun Liu and Lie Xu [105]. The Cat map is employed to scramble the pixel sequence of sub-images of the plain color image, and the DCT is utilized to change the value of the image in all distributions.

Recently, a triple-image-encryption and hiding scheme with chaos, compressive sensing (CS), and 3D DCT was presented by Xingyuan Wang and Cheng Liu [106]. They utilized 2D DWT to represent three grayscale plain images to obtain sparse matrices for scrambling. Then, a 2D infinite collapse map (ICM) was introduced to compress the scrambled matrices. Finally, 3D DCT was used to embed compressed matrices into a color carrier image to obtain the cipher image. Their scheme can simultaneously encrypt and embed three grayscale images into a color carrier image.

3.2. Chaos-Based Image Encryption Based on Asymmetric Encryption (Public Key Algorithm)

Symmetric cryptosystems, also known as single key cryptosystems, are known for their high efficiency. However, it is worth noting that the encryption and decryption parties must use the same key, which must be transmitted through a secure channel to prevent it from being leaked. Otherwise, the ciphertext may be breached. In contrast, asymmetric encryption structures do not have this concern. Unlike symmetric cryptosystems, asymmetric cryptosystems, also known as public key algorithms, have two keys: a public key and a private key. The public key and the private key are different keys, and a piece of information can be encrypted with the public key and then decrypted with the private key, or vice versa. The former is widely used for the sender to send secret information to the receiver, while the latter is widely utilized for the authentication of the sender during broadcast. Well-known public key cryptography algorithms include RSA, ElGamal, and elliptic curve cryptography algorithms. Figure 6 shows the general flow of image-encryption transmission based on a public key.

This section covers several approaches to asymmetric chaotic image encryption, including asymmetric algorithms based on chaos synchronization, chaotic image-encryption algorithms based on RSA, chaotic image-encryption algorithms based on elliptic curve, and other asymmetric image-encryption algorithms. These methods are discussed and researched to explore their potential for improving the security and efficiency of image encryption.

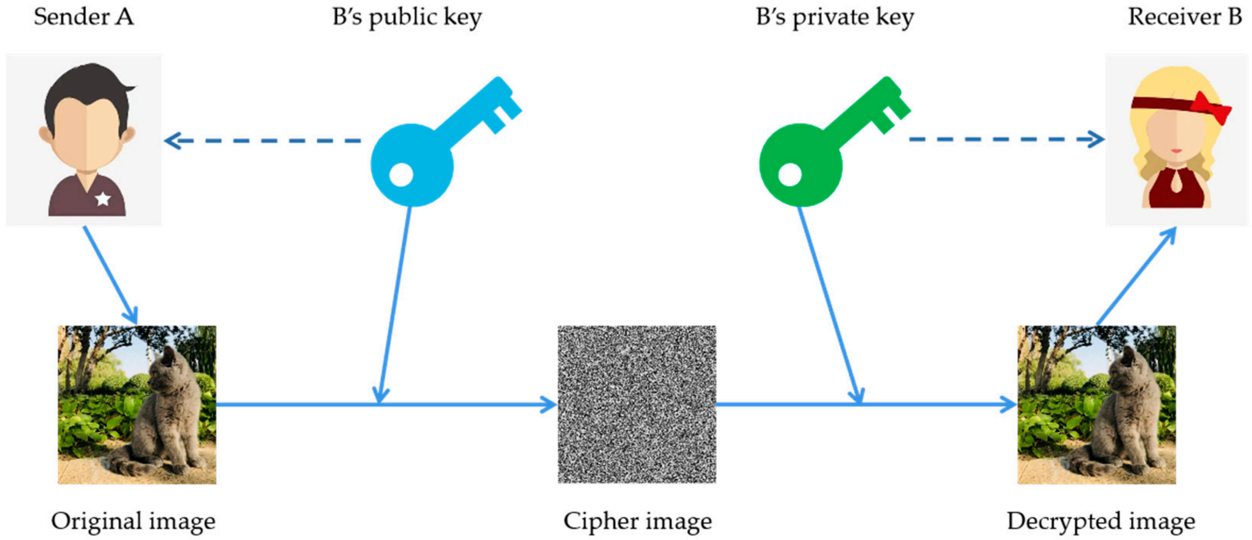

Figure 6. The general flow of image-encryption transmission based on a public key.

3.2.1. Chaotic-Synchronization-Based Asymmetric Image Encryption

In 2013, Chao-Jung Cheng and Chi-Bin Cheng [107] first introduced an asymmetric cryptosystem to chaos-based image encryption with the adaptive synchronization of an uncertain unified chaotic system and a cellular neural network. An adaptive controller with a parameter update law was constructed by them to asymptotically synchronize two chaotic systems. This synchronous controller was used in the image-encryption process to produce a pair of asymmetric keys for image encryption and decryption.

Zhengze Wu and Xiaohong Zhang [108] proposed an 8D generalized chaos synchronization (GCS) system which has complexity and irreversibility for asymmetric image encryption. It is implemented in Multisim^{TM} 14.0 circuit software. The GCS system was utilized for the secure communication of digital images. Given the intricate functional relationship between the drive and response systems, asymmetric encryption, which utilizes distinct keys and sequences held by the two parties involved in the communication, can be implemented. Additionally, data authentication can also be implemented.

3.2.2. RSA-Based Asymmetric Chaotic Image Encryption

The Rivest–Shamir–Adleman (RSA) algorithm, as the most famous and widely used asymmetric cryptosystem, has been gradually applied to chaotic image-encryption algorithms by a large number of researchers in recent years.

Ünal. C and Akif. A [109] designed a hybrid RSA (CRSA) encryption algorithm with a chaotic RNG. They also designed the circuit realization of chaotic system. This algorithm has the advantages of both RSA and chaotic systems.

In [110,111], although the specific methods are different, the RSA algorithm and Cat map are both used to construct the asymmetric image-encryption algorithm; these algorithms have high effectiveness, safety, and robustness.

Yujia Liu and Zhaoguo Jiang [112] combined RSA with a four-wing and Chen 4D hyperchaotic system to achieve optical image encryption. At the last step of the algorithm, the RSA is employed to asymmetrically encode the key to obtain the corresponding public key and private key.

Some scholars have tried to combine a hash function with the RSA algorithm to improve the security of image encryption. In Guodong Ye and Kaixin Jiao's article [113], the quantized Logistic map is employed to generate the keystreams. The RSA algorithm is used to confuse the plain image, then SHA-3 is utilized to compute the preprocessed image.

Recently, Guo-Dong Ye and Hui-Shan Wu [114] introduced a 3D ILM chaotic system, which has large key space and high complexity. Furthermore, a mathematical model of key acquisition (MKA) was also created. Then, the new system was combined with RSA for the asymmetric image encryption.

3.2.3. Elliptic-Curve-Based Asymmetric Chaotic Image Encryption

According to the needs of high security, short keys, and fast encryption speed, the elliptic curve (EC) public key cryptosystem is also a common public key encryption technique. Therefore, some image-encryption algorithms based on the EC and the chaotic system have been constructed by scholars.

Jiahui Wu and Xiaofeng [115] were the first, in 2017, to introduce an asymmetric image-encryption method based on the combination of an EC and chaotic system. The combination system of a 4D Cat map and the 3D Lorenz equation is employed for permutation and diffusion. Furthermore, it achieves the transmission of confidential information among multiple people with only small key groups and key numbers. Then it was improved by combining it with ElGamal and DNA technology, as the EC-ElGamal algorithm, in [116].

On the basic of the Diffie–Hellman key exchange technique, Dolendro and Manglem [117] presented a chaos-based image-encryption method whose keys are generated after sharing a random point on an elliptic curve.

3.2.4. Some Other Chaos-Based Asymmetric Chaotic Image-Encryption Methods

In Hongjun Liu and Abdurahman Kadir's asymmetric image-encryption algorithm [17], different receivers are distributed with different keys through a key-changing mechanism using a 2D discrete-time Henon map.

Hongjun Liu and Abdurahman Kadir [118] utilized Hash-512 in the plain image to generate the initial value and combined a four-wing complex chaotic system into their asymmetric image-encryption method. The components in red, yellow, and blue are sequentially preprocessed by a chaotic sequence for image encryption.

In Liansheng Sui and Kuaikuai Duan's articles [119,120], the asymmetric double (multiple) image encryptions based on fractional transform and a chaotic Logistic map are proposed. One is combined with Fourier transform while the other is bound to discrete fractional random transform.

Ali Shakiba [121] introduced a Chebyshev polynomial-based image-encryption algorithm with a chaotic PRNG to replicate a one-time pad. The key space of this algorithm was greatly expanded. Furthermore, it is secure enough to resist chosen-plaintext attack (CPA).

Jun Wang and Qinghua Wang [122] presented an asymmetric image-encryption algorithm with cylindrical diffraction random-phase encoding (DCRE) and reservation and truncation (PRT). In this scheme, DCRE is utilized to encrypt the plain image, then PRT is employed to separate the diffraction distribution of the complex amplitude into phase and amplitude parts, which are saved as asymmetric keys.

Yabin Zhang and Li Zhang [123] tried to blend several techniques into asymmetric image encryption, such as a hyperchaotic system, DNA level operation, Cat map, and phase-truncated fractional Fourier transform (ptFrFT). Furthermore, their method has strong resistance to the two-step iterative amplitude-phase retrieval algorithm.

3.3. Chaos-Based Image Encryption with Other Technology

In addition to the direct application of chaos to image encryption, chaotic systems can also be combined with other fields to encrypt images and take advantage of multiple technologies simultaneously. However, effective integration of these technologies requires further study. The different directions for combining chaotic systems with other technologies discussed in this section are shown in Figure 7.

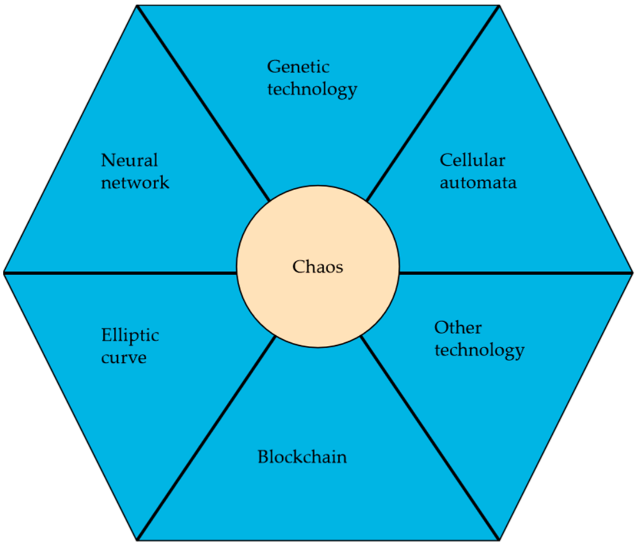

Figure 7. Directions for chaos to combine with other technologies.

3.3.1. Chaos-Based Image Encryption with Neural Networks

A neural network is a mathematical model of distributed parallel information processing that imitates the behavior characteristics of animal neural networks. This structure relies on the complexity of the system and achieves the purpose of processing information by adjusting the interconnection between a large number of internal nodes. Chaotic neural networks (CNNs), as the combination of chaos and neural networks, provide a new and promising direction for image encryption. By introducing chaotic systems into the learning and training processes of neural networks, CNNs can enhance the randomness and unpredictability of the network, making it more resistant to attacks and providing a higher degree of security. CNNs have been applied to a variety of image-encryption tasks, including image scrambling and watermarking, and have shown promising results. The combination of chaos and neural networks offers a promising avenue for further research and development in image encryption.

Shiguo Lian [124] was the first to propose a block-cipher-based encryption algorithm with a CNN. The diffusion phase is processed by a chaotic neuron layer and the confusion phase is implemented by a linear neuron layer. This structure has great security in computing but it may be vulnerable to attack because of its constant weight and bias matrices.

Based on [124], Nooshin Bigdeli and Yousef Farid [125] presented image encryption based on a chaotic neuron layer (CNL) and a permutation neuron layer (PNL), which consists of a three-input (the value of RGB), three-output (encoded streams) CNN. Three chaotic systems are employed to generate the weights and biases matrices of the CNL. The output of the CNL is the input of the PNL. Finally, rounds of permutation of data with linear permutation are combined with 2D nonlinear shuffling to achieve 3D permutation.

A Hopfield-CNN-based image-encryption approach was proposed by Xing-Yuan Wang and Zhi-Ming Li [126]. In a Hopfield CNN, every neuron's output signal is fed back to itself by other neurons. In the image-encryption phase, several chaotic maps, such as the Cat map and phased composite chaotic map, are employed for confusion. After confusion, a Hopfield CNN is utilized in the diffusion step.

Besides CNN, some researchers are trying to find neural networks with chaotic features for image encryption.

A construct called a fuzzy cellular neural network (FCNN) was introduced by K. Ratnavelu and M. Kalpana [127]. The value of FCNN parameters is identified to generate chaotic sequences for image encryption.

Liping Chen and Hao Yin [128,129] constructed a 3D fractional-order (FO) discrete Hopfield neural network (FODHNN), which has chaotic dynamics features, in the left Caputo discrete delta's sense. Then, the FODHNN was employed as a PRNG in image encryption.

Zhenlong Man and Jinqing Li [130] first tried to combine a convolutional neural network (CONN) and plaintext correlation scrambling mechanism and proposed double image encryption with a CONN and dynamic adaptive diffusion. They innovated in three main parts: Firstly, a bit-level split-fusion scheme was constructed. Then, a dual-channel encryption scheme for image was presented. Finally, a method of generating a plaintext-dependent chaotic scrambled pointer based on a CONN was designed.

The interspike interval (ISI) is the time between consecutive action potential peaks of a neuron, which is a crucial indicator for characterizing neural bursting. Ref. [131] constructed a discrete mHR model to produce four sets of hidden chaotic burst sequences, which are subsequently encoded using their ISIs. The encoded sequences exhibit higher complexity and better biological interpretability than the original burst sequences. The resulting encoded sequence is then used as an image-encryption scheme, providing greater resistance to a variety of attacks.

The original FHN neuron model is effective in theoretical analysis and numerical simulations but it has a high implementation cost. As a solution to this problem, ref. [132] proposed a multiplier-free implementation of a nonlinear function with N-shaped curves. Experimental results confirm that their approach can produce electrical activity with periodic spiking, chaotic, and quasi-periodic behavior, which suggests that it is suitable for implementing analog circuits for neuromorphic intelligence based on FHN neurons.

Junwei Suna and Chuangchuang Li [133] proposed a novel locally active hyperbolic memristor that can exhibit bistable phenomena. Using this memristor, they developed a Hindmarsh–Rose (HR)–FitzHugh–Nagumo (FN) HR neural network coupled by a hyperbolic memristor and examined the chaotic dynamics of the network under varying parameters and initial conditions. The HR-FN-HR model is comprised of a 2D FN neuron and two 2D HR neurons coupled by memory resistors. Experimental results show that this network has a more complex dynamic behavior compared to other neural networks. Furthermore, they proposed an image-encryption scheme based on this model. The study has significant theoretical implications for modeling the dynamic properties of biological neural systems.

3.3.2. Chaos-Based Image Encryption with Genetic Technology

Genetic technology is an optimization method that searches for the final solution among a group of potential solutions based on the principles of natural evolution. This process is repeated until a satisfactory solution is obtained. By combining genetic algorithms with chaotic systems, researchers have developed new and more efficient image-encryption algorithms that offer a high degree of security and can withstand attacks from potential adversaries. The combination of genetic technology and chaotic systems offers a promising approach to image encryption and optimization in general.

Abdul Hanan Abdullaha and Rasul Enayatifar [134] proposed a new image-encryption scheme based on both a chaotic Logistic map and genetic technology. They used genetic techniques to improve the chaos-based encryption algorithm, which was the first image-encryption method to use this genetic algorithm.

After that, many researchers have attempted to apply the combination of DNA methods and chaotic systems to image encryption. The basic idea of DNA-based image encryption consists of two parts. First, the plain image pixels are encoded into DNA sequences using DNA theory, and a key image is generated using DNA rules. In the second part, the key image is generated by the encoded plain image pixels based on DNA operation rules to obtain the cipher image. By combining DNA theory and chaotic systems, researchers have developed new and more effective image-encryption algorithms that offer a high degree of security and can withstand attacks from potential adversaries. The combination of DNA and chaotic systems offers a promising approach to image encryption and opens up new avenues for further research in this field.

Lili Liu and Qiang Zhang [135] were the first to use a combination of DNA encoding and a chaotic map in RGB image encryption. The DNA is utilized to encode the pixel values of image R, G, and B components and the Logistic map is used for n disturb image pixels. Then, an enhanced image-encryption algorithm based on a DNA sequence operation, image fusion, and a hyperchaos Chen system was proposed by Qiang Zhang and Ling Guo [136] based on [135].

Because of their extraordinary information density, DNA methods are an effective way to resolve the problem of the storage of one-time pads. Xing-Yuan Wang and Ying-Qian Zhang [137] combined a DNA method and a CML system to present an image-encryption method. Pseudo-random sequences generated by CML are used for XOR operation on pixels of the plain image. After that, they encoded the confused image with a DNA encoding rule and obtained a DNA matrix. Then, the rows and columns of the matrix were rearranged and confused. Finally, the DNA matrix was decoded by the DNA decoding rule to obtain the ciphered image.

Xiuli Chai [138] presented an image-encryption algorithm based on the chaotic system and DNA sequence operations. First, they used a DNA matrix to encode the plain image with a new wave-based permutation scheme, and then employed a chaotic sequence produced by a 2D Logistic chaotic map for row circular permutation (RCP) and column circular permutation (CCP).

Xiuli Chai and Xianglong Fu [139] presented a four-wing hyperchaos system and a DNA-encoding-based image-encryption scheme. They introduced a simultaneous intra-inter-component permutation mechanism dependent on the plaintext (SCPMDP) for shuffling, and a diffusion mechanism based on random numbers related to plaintext for diffusion.

Shijie Zhang and Lingfeng Liu [140] proposed a compound Sine-Piecewise Linear Chaotic Map (SPWLCM) to improve the dynamical complexity. Then, the SPWLCM and a DNA rule were used in their image-encryption algorithm. However, the rules of DNA encoding and decoding are determined by the SPWLCM, which is different from the previous studies.

Xinyu Gao and Bo Sun [141] proposed a color image-encryption algorithm based on cross-plane permutation, DNA mutation, and a hyperchaotic system. DNA mutation refers to the transformation of a short DNA sequence into another short sequence at an unknown site. It involves combining a simplified DNA mutation process with hyperchaotic sequences to enhance randomness, and permuting color images across planes to strengthen the security of the algorithm.

3.3.3. Chaos-Based Image Encryption with Cellular Automata

Cellular automata (CA) form a highly parallel and distributed system that is based on the idea that complex structures and processes in nature can be generated by the simple interaction of a large number of basic building blocks. CA can evolve through simple logical calculations and thus exhibit pseudo-random and complex behavior. The basic idea of CA is to divide a space into a grid of cells, with each cell being in one of a finite number of states. The state of each cell is determined by its neighboring cells according to a set of simple rules. These rules can be applied in a parallel and distributed manner, allowing for the efficient processing of large amounts of data. Thus, CA can be used in cryptosystems [142,143] or to generate random sequences [144]. Researchers have been inspired to combine CA with a chaotic system to construct new image-encryption algorithms.

Xingyuan Wang and Dapeng Luan [145] introduced firstly an image-encryption method based on the combination of reversible CA and a chaotic system. The Logistic map is used to generate pseudo-random sequences to shuffle and change the values of bits of each pixel in the permutation stage and reversible CA is employed in the diffusion stage to substitute pixels.

A hybrid model of DNA, CA, and chaotic-system-based image encryption was proposed by Rasul Enayatifar and Hossein Javedani Sadaei [146]. They converted pixels of the plain image into DNA nucleic acid using DNA standard rules. Then, the pixels were encoded with sequences generated by CA and standard rules, where the choice of the rules to be utilized was decided by a 2D Tinkerbell map.

In Abolfazl Yaghouti Niyat and Mohammad Hossein Moattar's article [147], a non-uniform CA framework with chaotic systems is proposed to solve the shortcomings of CA in cryptography. The Logistic map is used to initialize CA to create the key image, the Cat map is employed to generate chaotic sequences, and the Chen map is utilized to select keys from the key image.

3.3.4. Chaos-Based Image Encryption with Blockchain Technology

Due to the success of Bitcoin in recent years, blockchain technology has gained widespread attention from both industry and academia. As the core mechanism of Bitcoin, blockchain has many desirable attributes, including decentralization, anonymity, persistence, and auditability. In particular, blockchain can operate in a decentralized environment, enabling transactions to be decentralized, which helps to save costs and improve efficiency. Therefore, blockchain has great potential in the construction of future Internet systems [148]. The combination of blockchain and chaos for image encryption has also recently been studied by scholars.

To resist the CPA, Ruiping Li [149] presented a fingerprint-related image-encryption algorithm based on a chaotic system and the blockchain framework. The keystreams used do not rely on the original image, but on the fingerprint of the sender. This algorithm provides authentication and tracking capabilities in addition to CPA resistance.

In [150,151], the authors chose to introduce cloud storage or cloud computing into encryption algorithms. Ref. [150] proposed a blockchain-based Chaotic Deep Generative Adversarial Network Encryption (BCDGE) scheme with a cloud storage system for securing medical images. A Blockchain Chaotic and Paillier Map-Based Authentication (BC-PMA) scheme in a cloud computing environment was presented in [151] for security image data sharing. This scheme not only improves the accuracy of authentication but also reduces the false positive rate and calculation cost.

3.3.5. Chaos-Based Image Encryption with an Elliptic Curve

In addition to the applications for asymmetric image encryption discussed in Section 3.2.3, the elliptic curve has also been used by some scholars with symmetric chaotic image-encryption schemes.

In [152,153], Ahmed and Xiamu Niu hybridize a cyclic elliptic curve and a chaotic system to design faster and more secure image encryptions. Their research also inspired later scholars to pay attention to elliptic curves in chaotic image encryption.

Roayat. I. A [154] proposed a two-step image transmission method with a block-based elliptic curve (BBEC). The BBEC is employed in the first step in order to solve the problem of key distribution and management of symmetric key encryption. Then, a novel PRNG is used to generate a pseudo-random sequence for image encryption in step 2.

3.3.6. Chaos-Based Image Encryption with Some Other Technology

A scheme for image encryption using a digital signature was suggested by Aloka Sinha and Kehar Singh [155] in 2003. In this scheme, the digital signature of the original image is added to the encrypted version of the original image. They used Bose–Chaudhuri–Hocquenghem (BCH) code to encrypt the image, after which the digital signature was used to verify the validity of the image.

Zhengjun Liu and Qing Guo [156] proposed double image encryption based on a chaotic map and optical technology with gyrator transform. In this algorithm, the Logistic map is employed to generate the key, and the complex function is used to encode two plain images.

3.4. Review of the Chaos-Based Image-Encryption Algorithms with Outstanding Contributions

We review some outstanding contributions of chaotic image-encryption algorithms in Table 1.

Table 1. Review of the chaos-based image-encryption algorithms with outstanding contributions.

Year	Authors and Reference	Contribution	Label
1998	Jiri Fridrich [26]	A chaos-based image-encryption algorithm was proposed for the first time.	Symmetric Encryption
1998	Josef Scharinger [27]	They highlighted the PRNG role in image encryption.	Symmetric Encryption
2004	Guanrong Chen and Yaobin Mao [18]	They first extended Cat maps and images to 3D encryption at the same time.	Symmetric Encryption
2005	Linhua Zhang and Xiaofeng Liao [67]	They combined PLM with S-Box to apply image encryption.	Symmetric Encryption; S-Box
2006	K. Pareek Vinod [39]	They first proposed a chaotic color image-encryption algorithm.	Symmetric Encryption; Color image
2006	A. N. Pisarchik [90]	A spatiotemporal chaotic system was first applied to image encryption.	Symmetric Encryption; Spatiotemporal
2007	S. Kwok and Wallace K. S. Tang [84]	Chaotic image encryption based on a stream cipher was proposed for the first time.	Symmetric Encryption
2008	Tiegang Gao and Zengqiang Chen [61]	They first applied hyperchaotic systems to image-encryption algorithms	Symmetric Encryption; Hyperchaotic
2019	Lucas G. Nardo and Erivelton G [52]	The limited precision error was used as a source of randomness in a chaotic image-encryption algorithm.	Symmetric Encryption
2011	Zhi-liang ZhuWei Zhang [71]	A chaotic system was applied to image encryption at the bitplane level.	Symmetric Encryption; Bitplane
2016	Lu Xu and Zhi Li [100]	They combined PWLCM and BBD for image encryption.	Symmetric Encryption; Bitplane
2008	S. Behnia and A. Akhshani [55]	They used chaotic maps for image encryption after coupling for the first time.	Symmetric Encryption; Chaotification
2015	Xingyuan Wang and Lintao Liu [48]	The dynamic growth technique was introduced into a chaos-based image-encryption algorithm.	Symmetric Encryption; Chaotification
2019	Moatsum Alawida and Azman Samsudin [60]	TLTS and TSTS, formed using 1D chaotic systems as a seed map, were employed in image encryption.	Symmetric Encryption; Chaotification
2020	Zhongyun Hua and Zhihua Zhu [54]	They proposed LTMM-CIEA and used cross-planar arrangement and non-sequential diffusion.	Symmetric Encryption; Chaotification
2013	Chao-Jung Cheng and Chi-Bin Cheng [107]	They first applied asymmetric cryptography to chaotic image encryption.	Asymmetric Encryption
2017	Jiahui Wu and Xiaofeng Liao [115]	They first introduced an elliptic curve to a chaotic image-encryption algorithm.	Asymmetric Encryption
2017	Ünal. C and Akif. A [109]	They first introduced RSA into a chaotic image-encryption algorithm.	Asymmetric Encryption
2019	Ali Shakiba [121]	An asymmetric image-encryption algorithm based on Chebyshev polynomial.	Asymmetric Encryption
2009	Chun-jiang pang [102]	DWT-based frequency-domain chaotic image encryption was proposed for the first time.	Frequency Domain
2011	Zhengjun Liu and Lie Xu [105]	Chaotic color image encryption based on DCT.	Frequency Domain
2012	Abdul Hanan Abdullah [134]	It was the first time to combine chaotic system and gene technology for image encryption.	Genetic technology
2012	Lili Liu and Qiang Zhang [135]	A combination of DNA and chaotic systems for color image encryption.	Genetic technology
2017	Xiuli Chai [138]	They utilized a DNA matrix for image encryption while the chaotic system is for RCP and CCP.	Genetic technology
2009	Shiguo Lian [124]	Image encryption was carried out by combining neural networks with a chaotic system.	Neural networks
2013	Xingyuan Wang and Dapeng Luan [145]	Cellular automata were applied to a chaotic image-encryption scheme for the first time.	Cellular automata
2021	Ruiping Li [149]	The blockchain framework was used in chaotic image encryption.	Blockchain

While chaos-based image-encryption algorithms have been significantly improved and extended, there are still some shortcomings that need to be addressed in order to optimize their performance in certain aspects, such as resistance to attacks and processing of encrypted images. In Section 6 we discuss these challenges in more detail and explore potential solutions.

4. Security Evaluation of Image-Encryption Algorithms

A variety of image-encryption algorithms based on chaos have been proposed, and evaluation methods for their encryption performance, efficiency, security, and other aspects are also needed. Here we introduce some concepts of performance-testing methods [157] for chaotic image-encryption algorithms for readers to understand the relevant content.

- Key space

A good image-encryption algorithm should have strong key sensitivity, and its key space should be large enough to make brute force attacks impossible [18]. Generally speaking, a key space larger than 2^{128} is sufficient to prevent brute force cracking.

- Key sensitivity

Before being used for image encryption, a chaotic system needs to be tested for properties that are extremely sensitive to initial conditions. Key sensitivity means that even a small change in the key can lead to a considerable deviation from the correct result.

- Histogram

The histogram describes the distribution of image pixel values. In an ideal algorithm, the histogram should be smooth and the pixel values evenly distributed to prevent the leakage of image information.

- Correlation analysis

In general, there is a high correlation between adjacent pixels of a normal image. Therefore, in order to hide the original image information, it is necessary to encrypt the image and reduce the correlation of its adjacent pixels. We can judge whether the algorithm is complex enough by checking whether the adjacent pixels of the encrypted image are randomly distributed in the whole region.

- Information entropy (Shannon entropy)

Information entropy is used to measure the unpredictability and uncertainty of an information source. The higher the information entropy, the more uncertainty the information source has. The formula of information entropy can be written as:

$$I(T) = -\Sigma_{i=1}^{N} r(t_i)\ log_2\ r(t_i), \tag{13}$$

where $r(t_i)$ denotes the probability of symbol t_i in the information source T, and N is the cardinal number of symbols of information source T.

- Local information entropy

The local information entropy reflects the random distribution of the image in each local area. Its core idea is to divide the image into non-overlapping image blocks and calculate the average value of the information entropy.

- Unified average changing intensity (UACI)

UACI is a metric used to assess the quality of an image and is often used to compare the difference between the original image and the processed image. UACI is intended to measure the degree of change in the average brightness of an image and has the following equation:

$$\text{UACI} = \frac{1}{P}\left[\sum\nolimits_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{M}\right] \times 100\%, \tag{14}$$

where P is the number of pixels, M is the largest allowed pixel value in the images, and C_1 and C_2 are the input and encrypted image, respectively.

- Number of pixels change rate (NPCR)

NPCR is an index used to assess image-encryption algorithms and is usually used to compare the differences between images before and after encryption. NPCR is designed to measure the sensitivity of an encryption algorithm to an image and is formulated as follows:

$$\mathrm{NPCR} = \sum\nolimits_{i,j} \frac{d(i,j)}{S} \times 100\%, \tag{15}$$

where S is the total number pixels in the original image, and d is a binary array which is defined as:

$$d = \begin{cases} 1 & if\ C_1(i,j) \neq C_2(i,j) \\ 0 & if\ C_1(i,j) = C_2(i,j) \end{cases}, \tag{16}$$

where C_1 and C_2 are the input and encrypted images, respectively.

- Resistance to different attacks

In addition, the ability to withstand various attack methods is one of the important factors needed to evaluate the security of image-encryption algorithms. An excellent encryption program should be robust to all kinds of attacks, for example, known-plaintext attack, brute-force attack, statistical attack, ciphertext-only attack, and differential attack [157].

5. The Application Areas of Chaos-Based Image Encryption

The simulation implementation of chaotic systems is of great importance for engineering applications [158]. Various methods can be used to control the chaotic behavior of engineering systems, such as delayed feedback control, open-loop control, and bifurcation control, which involve manipulating the inputs or parameters of a system to stabilize its behavior. The developed principles and techniques in this regard have wide-ranging applications in aerospace, electrical engineering, mechanical engineering, robotics, cryptography, etc. The investigation shows that chaos-based image-encryption technology is mainly applied in the following three fields: medicine, the Internet of Things, and satellites.

5.1. Application of Chaos-Based Image Encryption in the Medical Field

Nowadays, with the progress of Internet technology, digital images are widely used in the medical field, and medical image communication is used in many applications such as remote surgery and remote diagnosis. Medical images generally contain confidential information, including private information, so the security of medical images is essential to protect users from all kinds of malicious attacks, avoid information loss, and ensure integrity. The method of applying chaos-based image encryption to medical images provides an effective way to achieve privacy protection and safe transmission of medical images.

In [159], a chaotic system and Hill cipher are utilized in mammography image encryption. The proposed approach uses a symmetric algorithm that can be employed in designing a FPGA-based encryption processor. A Logistic-map-based method was introduced in [160] for online secure medical image transmission on public networks. Akram Belazi and Muhammad Talha [161] combined DNA technology, a hash function, and chaotic systems to devise a medical image-encryption scheme. In [162], the authors presented a medical image-encryption framework with dynamic substitution boxes and chaotic maps for protecting patient privacy and medical records. Recently, Behrouz and Saleh [163] introduced an adaptive terminal sliding mode tracking approach for synchronization between sender and receiver. Subsequently, the synchronized chaotic systems are used in medical image encryption to improve security of transmission or storage.

Image-encryption algorithms for medical applications have specific requirements, such as high security, data integrity (image quality), and encryption/decryption speed. Traditional encryption schemes require high computational power and a long computation time, which may lead to considerable latency, and also have drawbacks such as low key space and vulnerability to attacks. The above scheme of applying chaos theory to medical image encryption has been tested during key space analysis, histogram analysis, correlation analysis, key sensitivity analysis, and testing of the ability to resist attack using UACI and NPCR to prove that it is secure enough to effectively solve the problems in secure medical communication.

5.2. Application of Chaos-Based Image Encryption in the Internet of Things (IoT) and Microcontroller Field

The Internet of Things is an extension and expansion of the network based on the Internet. It combines various information-sensing devices with the network to form a huge network, which can realize the interconnection of people, machines, and things at any time and in any place. Although the development of the IoT has gradually become routine in recent years, there are still many problems to be overcome in the aspects of technology, management, security, etc. Therefore, some researchers have tried to apply chaotic encryption algorithms to IoT to improve its security.

In [164,165], different chaotic systems such as the Cat map and Logistic map are applied to multimedia data encryption to improve its security. Jaishree and Arpit [166] are more interested in the future sixth generation of mobile cellular network (6G) technology. A hybrid image-encryption algorithm based on Hybridized Robust Zero-Watermarking and a hyperchaotic system along with RSA was presented by them to secure multimedia data communication over 6G networks in IoT.

Embedded systems have been applied in the military, electronic commerce, and many other fields. An embedded system is a kind of computer system used for specific applications, and the microcontroller is the mainstream component of the embedded system industry. The embedded microcontroller integrates the whole computer system into one chip, which has the characteristics of being monolithic, and having a small size, low power consumption, and high reliability.

Mihai Stanciu and Octaviana Datcu [167] first proposed a chaotic encryption algorithm implemented by an Atmel AVR microcontroller in 2012. However, it lacked an analysis of the safety performance.

M. A. Murilo-Escobar and C. Cruz-Hernandez [168] presented an improved chaotic encryption algorithm with high performance and low implementation-required resources and implemented it in an embedded 32-bit microcontroller. However, low chip memory, low frequency and speed, and no parallelism structure are the disadvantages of their scheme.

A lossless image-encryption algorithm using reversible lightweight operations was proposed by Siva Janakiraman and K Thenmozhi [169], in which the chaotic key was generated by a single-precision floating-point microcontroller. This approach solved the shortage of on-chip memory available for microcontrollers.

In [170], a secure algorithm with an application to encrypt digital images as confidential information for secure wireless communications on M2M systems was introduced to enhance the dynamics of five chaotic maps on microcontrollers. The article proved that according to the current computer capacity, using a chaotic map was sufficient to achieve security performance without affecting information security.

There are many reasons why chaotic image encryption can be suggested for microcontroller and IoT applications. First, the data transmitted by devices in the IoT and stored in microcontrollers may involve important information such as personal privacy information and trade secrets. These proposed solutions have been proven to be highly secure and confidential through the tests discussed in Section 4. Second, the chaotic image-encryption algorithm can be implemented in a simple circuit, which is ideal for use in embedded systems such as microcontrollers. In addition, the encryption/decryption speed of chaotic image-processing algorithms is extremely fast, and can thus meet the real-time requirements for data encryption and decryption in IoT.

5.3. Application of Chaos-Based Image Encryption in the Satellite Field

With the progress of science and technology and the development of the Internet, the application of satellite images and maps has become common. Artificial Earth satellites provide a higher working platform from the ground for a variety of sensors, so that the sensors have a broader field of vision. Now, satellite-based communications and remote sensing technologies can provide weather forecasting, geological surveys, resource management, and some other services. However, in the process of using satellite and remote sensing technology, the image will be threatened and lead to the loss of data privacy. Therefore, more and more attention is being paid to image security, and it is necessary to enforce security measures to ensure the authorized access of sensitive data.

In 2010, a chaotic satellite imagery cryptosystem with multiple chaotic systems, such as Tent, Logistic, Henon, and Chebyshev maps, was proposed by Muhammad Usama [171] to enhance the key space and security, and to overcome security, performance, privacy, and reliability issues of satellite imagery. Youcef Bentoutou and El-Habib Bensikaddour [172] combined a 2D Logistic-Adjusted-Sine (LAS) map with the classical counter mode of AES and presented a satellite image-encryption method that can resist SEU and transmission errors. Behrouz and Seyedeh [173] proposed a finite-time chaos synchronization satellite image-encryption method that utilized chaotic oscillators in both the transmitter and receiver ends. In their scheme, Lyapunov stability theory is combined with the finite-time synchronization concept to achieve finite-time synchronization.

Satellite communications face interference from multiple sources, and the overall stability of the chaotic system makes it resistant enough to deal with these interferences effectively. For example, it can increase the security and privacy of satellite image transmission, reduce errors in satellite image transmission, and use the synchronization properties of chaotic systems to synchronize multiple satellites, thus improving the stability and resistance capability of satellite communications. Since the above methods passed most of the assessments presented in Section 4, these approaches can make it secure enough to prevent hacking during satellite communication. Furthermore, these chaotic image-encryption algorithms applied to satellites also have a considerable advantage in encryption/decryption speed compared with the traditional methods.

6. The Challenges of Chaos-Based Image Encryption

Studying the current challenges of chaos-based image encryption is important for improving its various aspects and addressing potential vulnerabilities. By identifying these challenges, researchers can gain new insights and inspiration for developing new and more effective encryption techniques that can provide a high degree of security, efficiency, and usability. These challenges can be seen as opportunities for further research and development in the field of image encryption.

6.1. Resistance to Cryptanalysis or Attack

Chaos-based image-encryption technology has been developing rapidly, and its security, robustness, encryption efficiency, key space, and other attributes have been improved in different schemes with various methods. However, there is no absolutely secure encryption scheme, which is why many scholars have studied how to attack and improve various chaos-based image-encryption techniques. Therefore, protecting image-encryption algorithms from attacks is an important task and challenge in the field of image encryption.

Ref. [174] notes that all chaos-based image-encryption schemes using constant keys are vulnerable to attack. These systems can be made secure by having nonlinear functions of the system parameters or keys with time and state variables. Then, in order to benefit the subsequent chaotic cryptosystems, the common rules for security analysis of chaotic encryption are proposed in [157,175].

Rhouma and Safya [176] analyzed an image-encryption algorithm in [61] and used chosen-plaintext attack (CPA) and chosen-ciphertext attack (CCA) to attack it. The results show that only three couples of plaintext/ciphertext were enough to break the encryption in CPA and CCA.

The algorithm in [26], as one of the first chaos-based image-encryption algorithms, also proved to be unsafe from CCA in [177] by revealing the secret permutation method. The scheme was subsequently optimized in [178].

A CPA for S-Box-only chaotic image encryption was proposed by Yushu Zhang and Di Xiao [179], who pointed out that the computational complexity is only O (128L). The L here refers to the total number of pixels in the image.

An information-entropy-based chaotic image-encryption algorithm [180] was scrutinized in [181]. The analysis result shows that it is very insecure against differential attack.

Lidong Liu and Zhaolun Zhang [182] pointed out two vulnerabilities of the plaintext-related hyperchaotic encryption algorithm written by Zhen Li [183]; one is that there is no change in the gray value of a specific pixel in the diffusion process, and the other is that its arrangement is reversible.

6.2. Processing of an Encrypted Image

Processing encrypted images in schemes that use chaos-based image-encryption algorithms is a challenging task that requires the development of new techniques and approaches. In this regard, there are two main research directions that are currently being explored: image compression and image retrieval.

6.2.1. Image Compression

Image compression technology can reduce the number of bits describing the image so as to save the time required for image transmission and processing and reduce the occupied memory capacity. The general scheme has good compression performance, but it cannot guarantee the data confidentiality [184]. It is a challenging task to improve the security of images while ensuring the compression efficiency.

DWT and DCT are used respectively in two different chaos-based image-compression and encryption schemes in [103,184]. M. Brindha and N. Ammasai [185] utilized a hyperchaotic system to encrypt a plain image and compressed it with the Chinese remainder theorem to improve the compression ratio and security.

Subsequently, an elementary CA and block compressive sensing (BCS)-based chaotic image compression and encryption scheme was proposed by Xiuli Chai and Xianglong Fu [186]. The scheme can transmit the image securely and simultaneously compress it on a public network because of its excellent performance. However, it has a disadvantage that the entropy of information is not ideal.

Recently, Jiaqi Wang and Miao Zhang [187] introduced fractal coding and adaptive-thresholding sparsification into a chaotic image-encryption and compression algorithm. Besides its fractal compression time being shorter and its encryption efficiency being faster than those of some other algorithms, it can also process gray and color images of different sizes. However, its image reconstruction function has yet to be perfected.

An ordinary image-encryption scheme will occupy a large bandwidth of the image during transmission, but adopting a compression-based encryption scheme will increase time complexity. In order to balance encryption speed and transmission bandwidth, there is a need for compression while encrypting. In 2006, some scholars put forward the concept of compressed sensing [188], and introduced many algorithms that apply compressed sensing to image encryption.

In order to improve the security of encryption algorithms, several encryption algorithms combining chaotic systems with compressed sensing are proposed in [189–191]. The measurement matrix of compressed sensing is generated by the chaotic mapping, and then the original image is encrypted and compressed to obtain the final cipher image. For example, Yang Chen and Pan Ping [191] designed a new chaotic measurement matrix using Chebyshev mapping and Logistic mapping, and encrypted the measurement matrix through nonrepetitive scrambling and bidirectional diffusion algorithms, further improving the security of the encryption system. In reality, however, the quality of the decrypted image restored by the existing compressed sensing algorithm is not ideal. Determining how to construct better measurement matrices and image reconstruction algorithms is a further research direction for scholars.

6.2.2. Image Retrieval

Image retrieval is a type of pattern recognition that involves preprocessing (enhancement, restoration, compression, etc.), segmentation, and feature extraction of an image in order to classify it. To protect the image from theft during transmission, encryption is necessary during the feature extraction of private images. However, after the image is encrypted by an encryption algorithm, the data is in a disordered state, which makes it difficult to accurately perform feature extraction. Therefore, determining how to mine features suitable for classification, retrieval, and prediction from disordered data and retrieve images safely and efficiently in an encrypted domain are rather difficult and challenging research directions [192].

Although some excellent image retrieval schemes have been proposed in [193,194], they are all calculated for plaintext features, and their protection of image information is limited. Recently, Qing Zhang and Yong Yan [192] combined chaos-based image encryption with a deep learning model and realized the safe retrieval of images while effectively hiding the content information of the original image using a fusion method of a feature vector and ciphertext. However, a remaining deficiency is that the safety retrieval function of images with a small sample size is not perfect.

6.2.3. Selective Encryption of Images

Presently, most image-encryption research work is concentrated on encrypting the entire image to ensure the whole image is protected. However, in real-life scenarios, image owners may only need to safeguard some portion of the image, such as portrait or background information, when they want to share it. Thus, the selective encryption of image content is a relatively new and promising research direction [195–197].

Song [195] employed the YOLOv4 target detection model to identify the regions of interest and created a novel image-encryption algorithm using chaotic mapping. The proposed algorithm aims to protect local images. Similarly, Wang [196] utilized two different types of model, target detection and semantic segmentation, to obtain portrait information. They also developed a chaotic image-encryption algorithm that works well for images with non-uniform content sizes. Shan [197] used the PSPNet model to obtain portrait information in images and introduced a new chaotic image-encryption algorithm that used an upgraded perturbation–diffusion architecture. The experimental results indicated that this algorithm demonstrated good security performance.

6.2.4. Thumbnail-Preserving Encryption

In recent years, the increase in cloud storage has generated interest among researchers in image-encryption algorithms that offer a combination of confidentiality and usability. As a result, various schemes, including image annotation [198], image retrieval or searchable encryption [199], and thumbnail-holding encryption [200–202], have been proposed. Notably, thumbnail-preserving encryption has gained significant attention. While the first two schemes reduce the convenience of cloud storage, thumbnail-holding encryption enables users to identify target images easily as the ciphertext and plaintext have similar or identical thumbnails due to their a priori knowledge.

The combination of chaotic encryption and thumbnail-preserving encryption represents an optimal solution for balancing confidentiality and usability. Zhang [203] developed a novel two-dimensional chaotic system by combining logistic and sine functions and employed it in the creation of a thumbnail-preserving encryption technique that produced highly secure ciphertext images, even in the wake of known-plaintext attacks, data-loss attacks, and noise attacks. Utilizing a modified Logistic mapping, Zhu and Liu [204] constructed a point selection table that generated more disordered selected points, resulting in increased confidentiality of the ciphertext image in thumbnail-holdout encryption. Thus, the integration of chaotic encryption with thumbnail-preserving encryption is a critical area for future research in combining image confidentiality and usability.

7. Conclusions

Chaos-based image encryption is still one of the most effective methods for image encryption. This paper provides a detailed review and discussion of chaos-based image encryption, including symmetric and asymmetric encryption, to understand its development. A summary timeline and performance evaluation of image-encryption algorithms are also provided. Furthermore, the paper reviews the combination of chaotic systems with other technologies in image encryption, including neural networks, genetic algorithms, DNA technology, cellular automata, blockchain, elliptic curve, and other technologies. The unique attributes of chaos-based encryption, such as sensitivity to initial conditions, topological transitivity, and pseudo-randomness, enable cross-disciplinary collaborations and further improvements in image-encryption methods. Moreover, chaos-based image encryption plays a crucial role in practical applications. Examples of application scenarios, including the medical field, the Internet of Things, the microcontroller field, and the satellite field, are given in this paper. However, there are still some disadvantages and challenges in chaos-based image encryption. This paper mainly discusses two challenges: resistance to cryptanalysis or attack, and the processing of encrypted images. Nevertheless, these difficulties are not only challenges but also opportunities, which can encourage further research and development to supplement existing deficiencies and serve as future prospects for chaotic image encryption. Overall, chaos-based image encryption is a promising technique for image encryption, and ongoing research and development are necessary to improve its security, efficiency, and usability. By addressing challenges and exploring new opportunities, we can ensure the safety and confidentiality of sensitive information in an increasingly digital world.

Author Contributions: Conceptualization, L.L.; methodology, B.Z.; writing—original draft preparation, B.Z.; writing—review and editing, L.L.; funding acquisition, L.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China, grant number 62262039, and Outstanding Youth Foundation of Jiangxi Province, grant number 20212ACB212006.

Data Availability Statement: No new data were created. The images appeared in this article were all completed by the authors.

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

References

1. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
2. Li, T.-Y.; Yorke, J.A. Period three implies chaos. In *The Theory of Chaotic Attractors*; Springer: New York, NY, USA, 2004; pp. 77–84. [CrossRef]
3. May, R.M. Simple mathematical models with very complicated dynamics. *Nature* **1976**, *261*, 459–467. [CrossRef]
4. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
5. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
6. Matthews, R. On the derivation of a "chaotic" encryption algorithm. *Cryptologia* **1989**, *13*, 29–42. [CrossRef]
7. Sobhy, M.I.; Shehata, A.-E. Chaotic algorithms for data encryption. In Proceedings of the 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, Proceedings (Cat. No. 01CH37221), Salt Lake City, UT, USA, 7–11 May 2001; pp. 997–1000.
8. Zhang, X.; Chen, W. A new chaotic algorithm for image encryption. In Proceedings of the 2008 International Conference on Audio, Language and Image Processing, Shanghai, China, 7–9 July 2008; pp. 889–892.
9. Tang, G.; Wang, S.; Lü, H.; Hu, G. Chaos-based cryptograph incorporated with S-box algebraic operation. *Phys. Lett. A* **2003**, *318*, 388–398. [CrossRef]
10. Çavuşoğlu, Ü.; Kaçar, S.; Pehlivan, I.; Zengin, A. Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos Solitons Fractals* **2017**, *95*, 92–101. [CrossRef]
11. Liu, S.; Guo, C.; Sheridan, J.T. A review of optical image encryption techniques. *Opt. Laser Technol.* **2014**, *57*, 327–342. [CrossRef]

12. Chang, H.K.-C.; Liu, J.-L. A linear quadtree compression scheme for image encryption. *Signal Process. Image Commun.* **1997**, *10*, 279–290. [CrossRef]
13. Mira, C. *Chaotic Dynamics: From the One-Dimensional Endomorphism to the Two-Dimensional Diffeomorphism*; World Scientific: Singapore, 1987.
14. Avrutin, V.; Gardini, L.; Sushko, I.; Tramontana, F. *Continuous and Discontinuous Piecewise-Smooth One-Dimensional Maps: Invariant Sets and Bifurcation Structures*; World Scientific: Singapore, 2019.
15. Leonel Rocha, J.; Taha, A.-K. Allee's effect bifurcation in generalized logistic maps. *Int. J. Bifurc. Chaos* **2019**, *29*, 1950039. [CrossRef]
16. Amin, M.; Faragallah, O.S.; Abd El-Latif, A.A. A chaotic block cipher algorithm for image cryptosystems. *Commun. Nonlinear Sci. Numer. Simul.* **2010**, *15*, 3484–3497. [CrossRef]
17. Liu, H.; Kadir, A. Asymmetric color image encryption scheme using 2D discrete-time map. *Signal Process.* **2015**, *113*, 104–112. [CrossRef]
18. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [CrossRef]
19. Chen, G.; Ueta, T. Yet another chaotic attractor. *Int. J. Bifurc. Chaos* **1999**, *9*, 1465–1466. [CrossRef]
20. Rössler, O.E. An equation for continuous chaos. *Phys. Lett. A* **1976**, *57*, 397–398. [CrossRef]
21. Wolf, A.; Swift, J.B.; Swinney, H.L.; Vastano, J.A. Determining Lyapunov exponents from a time series. *Phys. D Nonlinear Phenom.* **1985**, *16*, 285–317. [CrossRef]
22. Chow, S.-N.; Hale, J.K. *Methods of Bifurcation Theory*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2012; Volume 251.
23. Pincus, S.M. Approximate entropy as a measure of system complexity. *Proc. Natl. Acad. Sci. USA* **1991**, *88*, 2297–2301. [CrossRef]
24. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; Booz-Allen and Hamilton Inc.: Mclean, VA, USA, 2001.
25. Scharinger, J.; Pichler, F. Efficient image encryption based on chaotic maps. In Proceedings of the 20th workshop of the Austrian Association for Pattern Recognition (OAGM/AAPR) on Pattern Recognition 1996, Munich, Germany, 30 June 1996; pp. 159–170.
26. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos* **1998**, *8*, 1259–1284. [CrossRef]
27. Scharinger, J. Fast encryption of image data using chaotic Kolmogorov flows. *J. Electron. Imaging* **1998**, *7*, 318–325. [CrossRef]
28. Li, C.; Luo, G.; Qin, K.; Li, C. An image encryption scheme based on chaotic tent map. *Nonlinear Dyn.* **2017**, *87*, 127–133. [CrossRef]
29. Xiang, T.; Liao, X.; Tang, G.; Chen, Y.; Wong, K.-W. A novel block cryptosystem based on iterating a chaotic map. *Phys. Lett. A* **2006**, *349*, 109–115. [CrossRef]
30. Miyamoto, M.; Tanaka, K.; Sugimura, T. Truncated Baker transformation and its extension to image encryption. In Proceedings of the Mathematics of Data/Image Coding, Compression, and Encryption II, Denver, CO, USA, 19–20 July 1999; pp. 13–25.
31. Yen, J.-C.; Guo, J.-I. Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation. *IEE Proc.-Vis. Image Signal Process.* **2000**, *147*, 167–175. [CrossRef]
32. Fridrich, J. Image encryption based on chaotic maps. In Proceedings of the 1997 IEEE International Conference on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation, Orlando, FL, USA, 12–15 October 1997; pp. 1105–1110.
33. Salleh, M.; Ibrahim, S.; Isnin, I.F. Enhanced chaotic image encryption algorithm based on Baker's map. In Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03, Bangkok, Thailand, 25–28 May 2003.
34. Lian, S.; Sun, J.; Wang, Z. A block cipher based on a suitable use of the chaotic standard map. *Chaos Solitons Fractals* **2005**, *26*, 117–129. [CrossRef]
35. Wong, K.-W.; Kwok, B.S.-H.; Law, W.-S. A fast image encryption scheme based on chaotic standard map. *Phys. Lett. A* **2008**, *372*, 2645–2652. [CrossRef]
36. Guan, Z.-H.; Huang, F.; Guan, W. Chaos-based image encryption algorithm. *Phys. Lett. A* **2005**, *346*, 153–157. [CrossRef]
37. Xiao, D.; Liao, X.; Wei, P. Analysis and improvement of a chaos-based image encryption algorithm. *Chaos Solitons Fractals* **2009**, *40*, 2191–2199. [CrossRef]
38. Baptista, M. Cryptography with chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [CrossRef]
39. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
40. Wang, Y.; Wong, K.-W.; Liao, X.; Chen, G. A new chaos-based fast image encryption algorithm. *Appl. Soft Comput.* **2011**, *11*, 514–522. [CrossRef]
41. Fouda, J.A.E.; Effa, J.Y.; Sabat, S.L.; Ali, M. A fast chaotic block cipher for image encryption. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 578–588. [CrossRef]
42. Nepomuceno, E.G.; Nardo, L.G.; Arias-Garcia, J.; Butusov, D.N.; Tutueva, A. Image encryption based on the pseudo-orbits from 1D chaotic map. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 061101. [CrossRef] [PubMed]
43. Mao, Y.; Chen, G.; Lian, S. A novel fast image encryption scheme based on 3D chaotic baker maps. *Int. J. Bifurc. Chaos* **2004**, *14*, 3613–3624. [CrossRef]
44. Wang, Y.; Wong, K.-W.; Liao, X.; Xiang, T.; Chen, G. A chaos-based image encryption algorithm with variable control parameters. *Chaos Solitons Fractals* **2009**, *41*, 1773–1783. [CrossRef]
45. Tong, X.; Cui, M. Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. *Signal Process.* **2009**, *89*, 480–491. [CrossRef]

46. Huang, X. Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dyn.* **2012**, *67*, 2411–2417. [CrossRef]
47. Ye, G.; Wong, K.-W. An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear Dyn.* **2012**, *69*, 2079–2087. [CrossRef]
48. Wang, X.; Liu, L.; Zhang, Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Opt. Lasers Eng.* **2015**, *66*, 10–18. [CrossRef]
49. Chen, J.-X.; Zhu, Z.-L.; Fu, C.; Yu, H.; Zhang, L.-B. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 846–860. [CrossRef]
50. Liu, L.; Miao, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus* **2016**, *5*, 289. [CrossRef] [PubMed]
51. Pak, C.; Huang, L. A new color image encryption using combination of the 1D chaotic map. *Signal Process.* **2017**, *138*, 129–137. [CrossRef]
52. Nardo, L.G.; Nepomuceno, E.G.; Arias-Garcia, J.; Butusov, D.N. Image encryption using finite-precision error. *Chaos Solitons Fractals* **2019**, *123*, 69–78. [CrossRef]
53. Santos, T.A.; Magalhães, E.P.; Basílio, N.P.; Nepomuceno, E.G.; Karimov, T.I.; Butusov, D.N. Improving Chaotic Image Encryption Using Maps with Small Lyapunov Exponents. In Proceedings of the 2020 Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, Russia, 11–13 March 2020; pp. 1–4.
54. Hua, Z.; Zhu, Z.; Yi, S.; Zhang, Z.; Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **2021**, *546*, 1063–1083. [CrossRef]
55. Behnia, S.; Akhshani, A.; Mahmodi, H.; Akhavan, A. A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos Solitons Fractals* **2008**, *35*, 408–419. [CrossRef]
56. Jafarizadeh, M.; Behnia, S. Hierarchy of chaotic maps with an invariant measure and their coupling. *Phys. D Nonlinear Phenom.* **2001**, *159*, 1–21. [CrossRef]
57. Jafarizadeh, M.; Behnia, S.; Khorram, S.; Nagshara, H. Hierarchy of chaotic maps with an invariant measure. *J. Stat. Phys.* **2001**, *104*, 1013–1028. [CrossRef]
58. Seyedzadeh, S.M.; Mirzakuchaki, S. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Process.* **2012**, *92*, 1202–1215. [CrossRef]
59. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.* **2014**, *97*, 172–182. [CrossRef]
60. Alawida, M.; Samsudin, A.; Teh, J.S.; Alkhawaldeh, R.S. A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* **2019**, *160*, 45–58. [CrossRef]
61. Gao, T.; Chen, Z. A new image encryption algorithm based on hyper-chaos. *Phys. Lett. A* **2008**, *372*, 394–400. [CrossRef]
62. Gao, T.; Chen, Z. Image encryption based on a new total shuffling algorithm. *Chaos Solitons Fractals* **2008**, *38*, 213–220. [CrossRef]
63. Zhu, C. A novel image encryption scheme based on improved hyperchaotic sequences. *Opt. Commun.* **2012**, *285*, 29–37. [CrossRef]
64. Zhu, H.; Zhao, C.; Zhang, X. A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem. *Signal Process. Image Commun.* **2013**, *28*, 670–680. [CrossRef]
65. Liu, W.; Sun, K.; Zhu, C. A fast image encryption algorithm based on chaotic map. *Opt. Lasers Eng.* **2016**, *84*, 26–36. [CrossRef]
66. Yu, F.; Xu, S.; Xiao, X.; Yao, W.; Huang, Y.; Cai, S.; Yin, B.; Li, Y. Dynamics analysis, FPGA realization and image encryption application of a 5D memristive exponential hyperchaotic system. *Integration* **2023**, *90*, 58–70. [CrossRef]
67. Zhang, L.; Liao, X.; Wang, X. An image encryption approach based on chaotic maps. *Chaos Solitons Fractals* **2005**, *24*, 759–765. [CrossRef]
68. Jolfaei, A.; Mirghadri, A. Image encryption using chaos and block cipher. *Comput. Inf. Sci.* **2011**, *4*, 172. [CrossRef]
69. Zhou, Q.; Wong, K.-W.; Liao, X.; Xiang, T.; Hu, Y. Parallel image encryption algorithm based on discretized chaotic map. *Chaos Solitons Fractals* **2008**, *38*, 1081–1092. [CrossRef]
70. Gu, G.; Han, G. An enhanced chaos based image encryption algorithm. In Proceedings of the First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06), Beijing, China, 30 August–1 September 2006; pp. 492–495.
71. Zhu, Z.-L.; Zhang, W.; Wong, K.-W.; Yu, H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **2011**, *181*, 1171–1186. [CrossRef]
72. Li, X.; Xie, Z.; Wu, J.; Li, T. Image encryption based on dynamic filtering and bit cuboid operations. *Complexity* **2019**, *2019*, 7485621. [CrossRef]
73. Xu, C.; Sun, J.; Wang, C. A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems. *Multimed. Tools Appl.* **2020**, *79*, 5573–5593. [CrossRef]
74. Xu, J.; Zhao, B.; Wu, Z. Research on color image encryption algorithm based on bit-plane and Chen Chaotic System. *Entropy* **2022**, *24*, 186. [CrossRef] [PubMed]
75. Song, W.; Fu, C.; Zheng, Y.; Tie, M.; Liu, J.; Chen, J. A parallel image encryption algorithm using intra bitplane scrambling. *Math. Comput. Simul.* **2023**, *204*, 71–88. [CrossRef]
76. Patidar, V.; Pareek, N.; Sud, K. A new substitution–diffusion based image cipher using chaotic standard and logistic maps. *Commun. Nonlinear Sci. Numer. Simul.* **2009**, *14*, 3056–3075. [CrossRef]
77. Huang, C.-K.; Nien, H.-H. Multi chaotic systems based pixel shuffle for image encryption. *Opt. Commun.* **2009**, *282*, 2123–2127. [CrossRef]

78. Kanso, A.; Ghebleh, M. A novel image encryption algorithm based on a 3D chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 2943–2959. [CrossRef]
79. Ying, W.; DeLing, Z.; Lei, J.; Yaoguang, W. The spatial-domain encryption of digital images based on high-dimension chaotic system. In Proceedings of the IEEE Conference on Cybernetics and Intelligent Systems, Singapore, 1–3 December 2004; pp. 1172–1176.
80. Gan, Z.-H.; Chai, X.-L.; Han, D.-J.; Chen, Y.-R. A chaotic image encryption algorithm based on 3-D bit-plane permutation. *Neural Comput. Appl.* **2019**, *31*, 7111–7130. [CrossRef]
81. Gao, H.; Zhang, Y.; Liang, S.; Li, D. A new chaotic algorithm for image encryption. *Chaos Solitons Fractals* **2006**, *29*, 393–399. [CrossRef]
82. Guo, J.-I. A new chaotic key-based design for image encryption and decryption. In Proceedings of the 2000 IEEE International Symposium on Circuits and Systems (ISCAS), Geneva, Switzerland, 28–31 May 2000; pp. 49–52.
83. Li, S.; Zheng, X. Cryptanalysis of a chaotic image encryption method. In Proceedings of the 2002 IEEE International Symposium on Circuits and Systems (ISCAS), Phoenix-Scottsdale, AZ, USA, 26–29 May 2002.
84. Kwok, H.; Tang, W.K. A fast image encryption system based on chaotic maps with finite precision representation. *Chaos Solitons Fractals* **2007**, *32*, 1518–1529. [CrossRef]
85. Liu, H.; Wang, X. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.* **2010**, *59*, 3320–3327. [CrossRef]
86. Mazloom, S.; Eftekhari-Moghadam, A.M. Color image encryption based on coupled nonlinear chaotic map. *Chaos Solitons Fractals* **2009**, *42*, 1745–1754. [CrossRef]
87. Liu, S.; Sun, J.; Xu, Z. An Improved Image Encryption Algorithm based on Chaotic System. *J. Comput.* **2009**, *4*, 1091–1100. [CrossRef]
88. Volos, C.K.; Kyprianidis, I.M.; Stouboulos, I.N. Image encryption process based on chaotic synchronization phenomena. *Signal Process.* **2013**, *93*, 1328–1340. [CrossRef]
89. Kaneko, K.; Tsuda, I. *Complex Systems: Chaos and Beyond: Chaos and Beyond: A Constructive Approach with Applications in Life Sciences*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2001.
90. Pisarchik, A.; Flores-Carmona, N.; Carpio-Valadez, M. Encryption and decryption of images with chaotic map lattices. *Chaos Interdiscip. J. Nonlinear Sci.* **2006**, *16*, 033118. [CrossRef] [PubMed]
91. Rhouma, R.; Meherzi, S.; Belghith, S. OCML-based colour image encryption. *Chaos Solitons Fractals* **2009**, *40*, 309–318. [CrossRef]
92. Xiang, T.; Wong, K.-W.; Liao, X. Selective image encryption using a spatiotemporal chaotic system. *Chaos Interdiscip. J. Nonlinear Sci.* **2007**, *17*, 023115. [CrossRef]
93. Sun, F.; Liu, S.; Li, Z.; Lü, Z. A novel image encryption scheme based on spatial chaos map. *Chaos Solitons Fractals* **2008**, *38*, 631–640. [CrossRef]
94. Zhang, Y.-Q.; Wang, X.-Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Inf. Sci.* **2014**, *273*, 329–351. [CrossRef]
95. Zhang, Y.-Q.; Wang, X.-Y. A new image encryption algorithm based on non-adjacent coupled map lattices. *Appl. Soft Comput.* **2015**, *26*, 10–20. [CrossRef]
96. Belkhouche, F.; Qidwai, U. Binary image encoding using 1D chaotic maps. In Proceedings of the Annual Technical Conference IEEE Region 5, New Orleans, LA, USA, 11 April 2003; pp. 39–43.
97. Xiao, H.-P.; Zhang, G.-J. An image encryption scheme based on chaotic systems. In Proceedings of the 2006 International Conference on Machine Learning and Cybernetics, Dalian, China, 13–16 August 2006; pp. 2707–2711.
98. Wang, X.; Wang, X.; Zhao, J.; Zhang, Z. Chaotic encryption algorithm based on alternant of stream cipher and block cipher. *Nonlinear Dyn.* **2011**, *63*, 587–597. [CrossRef]
99. Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun.* **2011**, *284*, 3895–3903. [CrossRef]
100. Xu, L.; Li, Z.; Li, J.; Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.* **2016**, *78*, 17–25. [CrossRef]
101. Luo, Y.; Du, M.; Liu, J. A symmetrical image encryption scheme in wavelet and time domain. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 447–460. [CrossRef]
102. Pang, C.-J. An image encryption algorithm based on discrete wavelet transform and two dimension cat mapping. In Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 25–26 April 2009; pp. 711–714.
103. Al-Maadeed, S.; Al-Ali, A.; Abdalla, T. A new chaos-based image-encryption and compression algorithm. *J. Electr. Comput. Eng.* **2012**, *2012*, 15. [CrossRef]
104. Wu, X.; Wang, D.; Kurths, J.; Kan, H. A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inf. Sci.* **2016**, *349*, 137–153. [CrossRef]
105. Liu, Z.; Xu, L.; Liu, T.; Chen, H.; Li, P.; Lin, C.; Liu, S. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Opt. Commun.* **2011**, *284*, 123–128. [CrossRef]
106. Wang, X.; Liu, C.; Jiang, D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Inf. Sci.* **2021**, *574*, 505–527. [CrossRef]

107. Cheng, C.-J.; Cheng, C.-B. An asymmetric image cryptosystem based on the adaptive synchronization of an uncertain unified chaotic system and a cellular neural network. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 2825–2837. [CrossRef]
108. Wu, Z.; Zhang, X.; Zhong, X. Generalized chaos synchronization circuit simulation and asymmetric image encryption. *IEEE Access* **2019**, *7*, 37989–38008. [CrossRef]
109. Çavuşoğlu, Ü.; Akgül, A.; Zengin, A.; Pehlivan, I. The design and implementation of hybrid RSA algorithm using a novel chaos based RNG. *Chaos Solitons Fractals* **2017**, *104*, 655–667. [CrossRef]
110. Jiao, K.; Ye, G.; Dong, Y.; Huang, X.; He, J. Image encryption scheme based on a generalized Arnold map and RSA algorithm. *Secur. Commun. Netw.* **2020**, *2020*, 9721675. [CrossRef]
111. Xu, Q.; Sun, K.; Zhu, C. A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map. *Phys. Scr.* **2020**, *95*, 035223. [CrossRef]
112. Liu, Y.; Jiang, Z.; Xu, X.; Zhang, F.; Xu, J. Optical image encryption algorithm based on hyper-chaos and public-key cryptography. *Opt. Laser Technol.* **2020**, *127*, 106171. [CrossRef]
113. Ye, G.; Jiao, K.; Huang, X. Quantum logistic image encryption algorithm based on SHA-3 and RSA. *Nonlinear Dyn.* **2021**, *104*, 2807–2827. [CrossRef]
114. Ye, G.-D.; Wu, H.-S.; Huang, X.-L.; Tan, S.-Y. Asymmetric image encryption algorithm based on a new 3D-ILM chaotic map. *Chin. Phys. B* **2022**, *32*, 030504. [CrossRef]
115. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **2017**, *90*, 225–237. [CrossRef]
116. Luo, Y.; Ouyang, X.; Liu, J.; Cao, L. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access* **2019**, *7*, 38507–38522. [CrossRef]
117. Laiphrakpam, D.S.; Khumanthem, M.S. A robust image encryption scheme based on chaotic system and elliptic curve over finite field. *Multimed. Tools Appl.* **2018**, *77*, 8629–8652. [CrossRef]
118. Liu, H.; Kadir, A.; Li, Y. Asymmetric color pathological image encryption scheme based on complex hyper chaotic system. *Optik* **2016**, *127*, 5812–5819. [CrossRef]
119. Sui, L.; Duan, K.; Liang, J.; Zhang, Z.; Meng, H. Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. *Opt. Lasers Eng.* **2014**, *62*, 139–152. [CrossRef]
120. Sui, L.; Duan, K.; Liang, J.; Hei, X. Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. *Opt. Express* **2014**, *22*, 10605–10621. [CrossRef]
121. Shakiba, A. A randomized CPA-secure asymmetric-key chaotic color image encryption scheme based on the Chebyshev mappings and one-time pad. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *33*, 562–571. [CrossRef]
122. Wang, J.; Wang, Q.-H.; Hu, Y. Asymmetric color image cryptosystem using detour cylindrical-diffraction and phase reservation & truncation. *IEEE Access* **2018**, *6*, 53976–53983.
123. Zhang, Y.; Zhang, L.; Zhong, Z.; Yu, L.; Shan, M.; Zhao, Y. Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation. *Opt. Lasers Eng.* **2021**, *143*, 106626. [CrossRef]
124. Lian, S. A block cipher based on chaotic neural networks. *Neurocomputing* **2009**, *72*, 1296–1301. [CrossRef]
125. Bigdeli, N.; Farid, Y.; Afshar, K. A novel image encryption/decryption scheme based on chaotic neural networks. *Eng. Appl. Artif. Intell.* **2012**, *25*, 753–765. [CrossRef]
126. Wang, X.-Y.; Li, Z.-M. A color image encryption algorithm based on Hopfield chaotic neural network. *Opt. Lasers Eng.* **2019**, *115*, 107–118. [CrossRef]
127. Ratnavelu, K.; Kalpana, M.; Balasubramaniam, P.; Wong, K.; Raveendran, P. Image encryption method based on chaotic fuzzy cellular neural networks. *Signal Process.* **2017**, *140*, 87–96. [CrossRef]
128. Chen, L.; Yin, H.; Huang, T.; Yuan, L.; Zheng, S.; Yin, L. Chaos in fractional-order discrete neural networks with application to image encryption. *Neural Netw.* **2020**, *125*, 174–184. [CrossRef]
129. Chen, L.-P.; Yin, H.; Yuan, L.-G.; Lopes, A.M.; Machado, J.T.; Wu, R.-C. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations. *Front. Inf. Technol. Electron. Eng.* **2020**, *21*, 866–879. [CrossRef]
130. Man, Z.; Li, J.; Di, X.; Sheng, Y.; Liu, Z. Double image encryption algorithm based on neural network and chaos. *Chaos Solitons Fractals* **2021**, *152*, 111318. [CrossRef]
131. Bao, H.; Hua, Z.; Liu, W.; Bao, B. Discrete memristive neuron model and its interspike interval-encoded application in image encryption. *Sci. China Technol. Sci.* **2021**, *64*, 2281–2291. [CrossRef]
132. Xu, Q.; Chen, X.; Chen, B.; Wu, H.; Li, Z.; Bao, H. Dynamical analysis of an improved FitzHugh-Nagumo neuron model with multiplier-free implementation. *Nonlinear Dyn.* **2023**, *111*, 8737–8749. [CrossRef]
133. Sun, J.; Li, C.; Wang, Z.; Wang, Y. Dynamic analysis of HR-FN-HR neural network coupled by locally active hyperbolic memristors and encryption application based on Knuth-Durstenfeld algorithm. *Appl. Math. Model.* **2023**, *121*, 463–483. [CrossRef]
134. Abdullah, A.H.; Enayatifar, R.; Lee, M. A hybrid genetic algorithm and chaotic function model for image encryption. *AEU-Int. J. Electron. Commun.* **2012**, *66*, 806–816. [CrossRef]
135. Liu, L.; Zhang, Q.; Wei, X. A RGB image encryption algorithm based on DNA encoding and chaos map. *Comput. Electr. Eng.* **2012**, *38*, 1240–1248. [CrossRef]

136. Zhang, Q.; Guo, L.; Wei, X. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Opt.-Int. J. Light Electron Opt.* **2013**, *124*, 3596–3600. [CrossRef]
137. Wang, X.-Y.; Zhang, Y.-Q.; Bao, X.-M. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Lasers Eng.* **2015**, *73*, 53–61. [CrossRef]
138. Chai, X.; Chen, Y.; Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **2017**, *88*, 197–213. [CrossRef]
139. Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **2019**, *155*, 44–62. [CrossRef]
140. Zhang, S.; Liu, L. A novel image encryption algorithm based on SPWLCM and DNA coding. *Math. Comput. Simul.* **2021**, *190*, 723–744. [CrossRef]
141. Gao, X.; Sun, B.; Cao, Y.; Banerjee, S.; Mou, J. A color image encryption algorithm based on hyperchaotic map and DNA mutation. *Chin. Phys. B* **2022**, *32*, 030501. [CrossRef]
142. Sen, S.; Shaw, C.; Chowdhuri, D.R.; Ganguly, N.; Chaudhuri, P.P. Cellular automata based cryptosystem (CAC). In Proceedings of the Information and Communications Security: 4th International Conference, ICICS, Singapore, 9–12 December 2002; pp. 303–314.
143. Abdo, A.; Lian, S.; Ismail, I.A.; Amin, M.; Diab, H. A cryptosystem based on elementary cellular automata. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 136–147. [CrossRef]
144. Wolfram, S. Random sequence generation by cellular automata. *Adv. Appl. Math.* **1986**, *7*, 123–169. [CrossRef]
145. Wang, X.; Luan, D. A novel image encryption algorithm using chaos and reversible cellular automata. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 3075–3085. [CrossRef]
146. Enayatifar, R.; Sadaei, H.J.; Abdullah, A.H.; Lee, M.; Isnin, I.F. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Opt. Lasers Eng.* **2015**, *71*, 33–41. [CrossRef]
147. Wu, J.; Liao, X.; Yang, B. Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. *Signal Process.* **2017**, *141*, 109–124. [CrossRef]
148. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
149. Li, R. Fingerprint-related chaotic image encryption scheme based on blockchain framework. *Multimed. Tools Appl.* **2021**, *80*, 30583–30603. [CrossRef]
150. Neela, K.; Kavitha, V. Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. *Appl. Intell.* **2022**, *53*, 4733–4747. [CrossRef]
151. Singh, C.E.J.; Sunitha, C.A. Chaotic and Paillier secure image data sharing based on blockchain and cloud security. *Expert Syst. Appl.* **2022**, *198*, 116874. [CrossRef]
152. El-Latif, A.A.A.; Li, L.; Niu, X. A new image encryption scheme based on cyclic elliptic curve and chaotic system. *Multimed. Tools Appl.* **2014**, *70*, 1559–1584. [CrossRef]
153. Abd El-Latif, 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]
154. Abdelfatah, R.I. Secure image transmission using chaotic-enhanced elliptic curve cryptography. *IEEE Access* **2019**, *8*, 3875–3890. [CrossRef]
155. Sinha, A.; Singh, K. A technique for image encryption using digital signature. *Opt. Commun.* **2003**, *218*, 229–234. [CrossRef]
156. Liu, Z.; Guo, Q.; Xu, L.; Ahmad, M.A.; Liu, S. Double image encryption by using iterative random binary encoding in gyrator domains. *Opt. Express* **2010**, *18*, 12033–12043. [CrossRef] [PubMed]
157. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
158. Chen, G. *Controlling Chaos and Bifurcations in Engineering Systems*; CRC Press: Boca Raton, FL, USA, 1999.
159. Naveenkumar, S.; Panduranga, H. Chaos and hill cipher based image encryption for mammography images. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 1–5.
160. Mostafa, S.; Fahim, M.A.N.I.; Hossain, A.A. A new chaos based medical image encryption scheme. In Proceedings of the 2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT), Himeji, Japan, 1–3 September 2017; pp. 1–6.
161. Belazi, A.; Talha, M.; Kharbech, S.; Xiang, W. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access* **2019**, *7*, 36667–36681. [CrossRef]
162. Ibrahim, S.; Alhumyani, H.; Masud, M.; Alshamrani, S.S.; Cheikhrouhou, O.; Muhammad, G.; Hossain, M.S.; Abbas, A.M. Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps. *IEEE Access* **2020**, *8*, 160433–160449. [CrossRef]
163. Vaseghi, B.; Mobayen, S.; Hashemi, S.S.; Fekih, A. Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption. *IEEE Access* **2021**, *9*, 25911–25925. [CrossRef]
164. Boutros, A.; Hesham, S.; Georgey, B. Hardware acceleration of novel chaos-based image encryption for IoT applications. In Proceedings of the 2017 29th International Conference on Microelectronics (ICM), Beirut, Lebanon, 10–13 December 2017; pp. 1–4.

165. Nath, S.; Som, S.; Negi, M. Lca approach for image encryption based on chaos to secure multimedia data in iot. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019; pp. 410–416.
166. Jain, J.; Jain, A.; Srivastava, S.K.; Verma, C.; Raboaca, M.S.; Illés, Z. Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA. *Mathematics* **2022**, *10*, 1071. [CrossRef]
167. Stanciu, M.; Datcu, O. Atmel AVR microcontroller implementation of a new enciphering algorithm based on a chaotic Generalized Hénon Map. In Proceedings of the 2012 9th International Conference on Communications (COMM), Bucharest, Romania, 21–23 June 2012; pp. 319–322.
168. Murillo-Escobar, M.A.; Cruz-Hernández, C.; Abundiz-Pérez, F.; López-Gutiérrez, R.M. Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller. *Microprocess. Microsyst.* **2016**, *45*, 297–309. [CrossRef]
169. Janakiraman, S.; Thenmozhi, K.; Rayappan, J.B.B.; Amirtharajan, R. Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller. *Microprocess. Microsyst.* **2018**, *56*, 1–12. [CrossRef]
170. García-Guerrero, E.; Inzunza-González, E.; López-Bonilla, O.; Cárdenas-Valdez, J.; Tlelo-Cuautle, E. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. *Chaos Solitons Fractals* **2020**, *133*, 109646. [CrossRef]
171. Usama, M.; Khan, M.K.; Alghathbar, K.; Lee, C. Chaos-based secure satellite imagery cryptosystem. *Comput. Math. Appl.* **2010**, *60*, 326–337. [CrossRef]
172. Bentoutou, Y.; Bensikaddour, E.-H.; Taleb, N.; Bounoua, N. An improved image encryption algorithm for satellite applications. *Adv. Space Res.* **2020**, *66*, 176–192. [CrossRef]
173. Vaseghi, B.; Hashemi, S.S.; Mobayen, S.; Fekih, A. Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems. *IEEE Access* **2021**, *9*, 21332–21344. [CrossRef]
174. Sobhy, M.I.; Shehata, A.-E. Methods of attacking chaotic encryption and countermeasures. In Proceedings of the 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, Proceedings (Cat. No. 01CH37221), Salt Lake City, UT, USA, 7–11 May 2001; pp. 1001–1004.
175. Alvarez, G.; Amigó, J.M.; Arroyo, D.; Li, S. Lessons learnt from the cryptanalysis of chaos-based ciphers. *Chaos-Based Cryptogr. Theory Algorithms Appl.* **2011**, *42*, 257–295.
176. Rhouma, R.; Belghith, S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. *Phys. Lett. A* **2008**, *372*, 5973–5978. [CrossRef]
177. Solak, E.; Cokal, C.; Yildiz, O.T.; Biyikoğlu, T. Cryptanalysis of Fridrich's chaotic image encryption. *Int. J. Bifurc. Chaos* **2010**, *20*, 1405–1413. [CrossRef]
178. Xie, E.Y.; Li, C.; Yu, S.; Lü, J. On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Process.* **2017**, *132*, 150–154. [CrossRef]
179. Zhang, Y.; Xiao, D. Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack. *Nonlinear Dyn.* **2013**, *72*, 751–756. [CrossRef]
180. Ye, G.; Pan, C.; Huang, X.; Zhao, Z.; He, J. A chaotic image encryption algorithm based on information entropy. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850010. [CrossRef]
181. Li, C.; Lin, D.; Feng, B.; Lü, J.; Hao, F. Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *IEEE Access* **2018**, *6*, 75834–75842. [CrossRef]
182. Liu, L.; Zhang, Z.; Chen, R. Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos. *IEEE Access* **2019**, *7*, 126450–126463. [CrossRef]
183. Li, Z.; Peng, C.; Li, L.; Zhu, X. A novel plaintext-related image encryption scheme using hyper-chaotic system. *Nonlinear Dyn.* **2018**, *94*, 1319–1333. [CrossRef]
184. Yuen, C.-H.; Wong, K.-W. A chaos-based joint image compression and encryption scheme using DCT and SHA-1. *Appl. Soft Comput.* **2011**, *11*, 5092–5098. [CrossRef]
185. Brindha, M.; Gounden, N.A. A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem. *Appl. Soft Comput.* **2016**, *40*, 379–390. [CrossRef]
186. Chai, X.; Fu, X.; Gan, Z.; Zhang, Y.; Lu, Y.; Chen, Y. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. *Neural Comput. Appl.* **2020**, *32*, 4961–4988. [CrossRef]
187. Wang, J.; Zhang, M.; Tong, X.; Wang, Z. A chaos-based image compression and encryption scheme using fractal coding and adaptive-thresholding sparsification. *Phys. Scr.* **2022**, *97*, 105201. [CrossRef]
188. Candès, E.J.; Romberg, J.; Tao, T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inf. Theory* **2006**, *52*, 489–509. [CrossRef]
189. Xiao, D.; Deng, M.; Zhu, X. A reversible image authentication scheme based on compressive sensing. *Multimed. Tools Appl.* **2015**, *74*, 7729–7752. [CrossRef]
190. Zhang, Y.; Zhou, J.; Chen, F.; Zhang, L.Y.; Wong, K.-W.; He, X.; Xiao, D. Embedding cryptographic features in compressive sensing. *Neurocomputing* **2016**, *205*, 472–480. [CrossRef]
191. Yang, C.; Pan, P.; Ding, Q. Image encryption scheme based on mixed chaotic bernoulli measurement matrix block compressive sensing. *Entropy* **2022**, *24*, 273. [CrossRef] [PubMed]

192. Zhang, Q.; Yan, Y.; Lin, Y.; Li, Y. Image Security Retrieval Based on Chaotic Algorithm and Deep Learning. *IEEE Access* **2022**, *10*, 67210–67218. [CrossRef]
193. Yue-Hei Ng, J.; Yang, F.; Davis, L.S. Exploiting local features from deep networks for image retrieval. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Boston, MA, USA, 7–12 June 2015; pp. 53–61.
194. Gordo, A.; Almazán, J.; Revaud, J.; Larlus, D. Deep image retrieval: Learning global representations for image search. In Proceedings of the Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, 11–14 October 2016; pp. 241–257.
195. Song, W.; Fu, C.; Zheng, Y.; Cao, L.; Tie, M.; Sham, C.-W. Protection of image ROI using chaos-based encryption and DCNN-based object detection. *Neural Comput. Appl.* **2022**, *34*, 5743–5756. [CrossRef]
196. Wang, J.; Liu, L.; Xu, M.; Li, X. A novel content-selected image encryption algorithm based on the LS chaotic model. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 8245–8259. [CrossRef]
197. Shan, Y.; He, M.; Yu, Z.; Wu, H. Pixel level Image Encryption Based on Semantic Segmentation. In Proceedings of the 2018 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO), Prague, Czech Republic, 19–21 May 2018; pp. 147–152.
198. Hanbury, A. A survey of methods for image annotation. *J. Vis. Lang. Comput.* **2008**, *19*, 617–627. [CrossRef]
199. Radenović, F.; Tolias, G.; Chum, O. Fine-tuning CNN image retrieval with no human annotation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *41*, 1655–1668. [CrossRef]
200. Yang, C.-H.; Weng, C.-Y.; Yang, Y.-Z. TPEIP: Thumbnail preserving encryption based on sum preserving for image privacy. *J. Inf. Secur. Appl.* **2022**, *70*, 103352. [CrossRef]
201. Tajik, K.; Gunasekaran, A.; Dutta, R.; Ellis, B.; Bobba, R.B.; Rosulek, M.; Wright, C.V.; Feng, W.-C. Balancing Image Privacy and Usability with Thumbnail-Preserving Encryption. *IACR Cryptol. Eprint Arch.* **2019**, *2019*, 295.
202. Zhang, Y.; Zhao, R.; Xiao, X.; Lan, R.; Liu, Z.; Zhang, X. HF-TPE: High-fidelity thumbnail-preserving encryption. *IEEE Trans. Circuits Syst. Video Technol.* **2021**, *32*, 947–961. [CrossRef]
203. Zhang, Y.; Zhao, R.; Zhang, Y.; Lan, R.; Chai, X. High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 2993–3010. [CrossRef]
204. Zhu, Z.; Liu, L. Thumbnail-preserving encryption based on improved logistic system. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 10167–10179. [CrossRef]

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.