applied system innovation

Review

Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap

Behrouz Zolfaghari [1,*] and Takeshi Koshiba [2]

[1] Cyber Science Lab, University of Guelph, Guelph, ON N1G 2W1, Canada
[2] Department of Integrated Arts and Sciences, Waseda University, Tokyo 169-8050, Japan; tkoshiba@waseda.jp
* Correspondence: behrouz@cybersciencelab.org

Abstract: Recently, many researchers have been interested in the application of chaos in cryptography. Specifically, numerous research works have been focusing on chaotic image encryption. A comprehensive survey can highlight existing trends and shed light on less-studied topics in the area of chaotic image encryption. In addition to such a survey, this paper studies the main challenges in this field, establishes an ecosystem for chaotic image encryption, and develops a future roadmap for further research in this area.

Keywords: image encryption; chaos; chaotic encryption; chaotic image encryption; trend analysis; future roadmap

Citation: Zolfaghari, B.; Koshiba, T. Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap. *Appl. Syst. Innov.* **2022**, *5*, 57. https://doi.org/10.3390/asi5030057

Received: 23 May 2022
Accepted: 7 June 2022
Published: 13 June 2022

1. Introduction

Image processing is used in various computing environments [1,2]. Image processing techniques take advantage of different security mechanisms. Among these mechanisms, in this paper, we focus on encryption, which has been of critical importance in image processing [3], as well as many other areas [4–6].

In recent years, the cryptography research community has taken advantage of the advancements in different technologies and theories including information theory [7], quantum computing [8], neural computing [9], Very Large Scale Integration (VLSI) technology [10], and especially, chaos theory [11].

All the above-mentioned theories have especially affected image encryption. However, in this paper, we are specifically interested in the applications of chaos theory in image encryption. Chaos is the characteristic of a system whose current state is guaranteed to be highly sensitive to the previous state (spatial chaos), the initial conditions (temporal chaos), or both (spatio-temporal chaos). Such a sensitivity makes the output or the behavior of a chaotic system difficult to predict. Chaos theory justifies and formulates the apparent disorder of chaotic systems on the basis of orderly patterns, structured feedback loops, iterative repetitions, self-organization, self-similarity, fractals, etc. Chaotic maps, attractors, and sequences all refer to the mathematical structures used for this formulation. Chaotic systems, maps, attractors, and sequences have been of great interest to the research community in recent years [12,13]. They have been used for security purposes in a broad variety of applications ranging from smart grids [14] to communication systems [15]. Especially, chaotic encryption has been used for encrypting a variety of content types in addition to images [1,2].

Figure 1 illustrates how image encryption converges with chaos theory at chaotic image encryption.

Figure 1 first of all introduces the icons we will use in the rest of this paper to represent *image processing, encryption, image encryption, chaos, and chaotic image encryption.* Furthermore, this figure shows how image processing joins encryption and then chaos theory to build *chaotic image encryption* as a branch of science and a field of research.

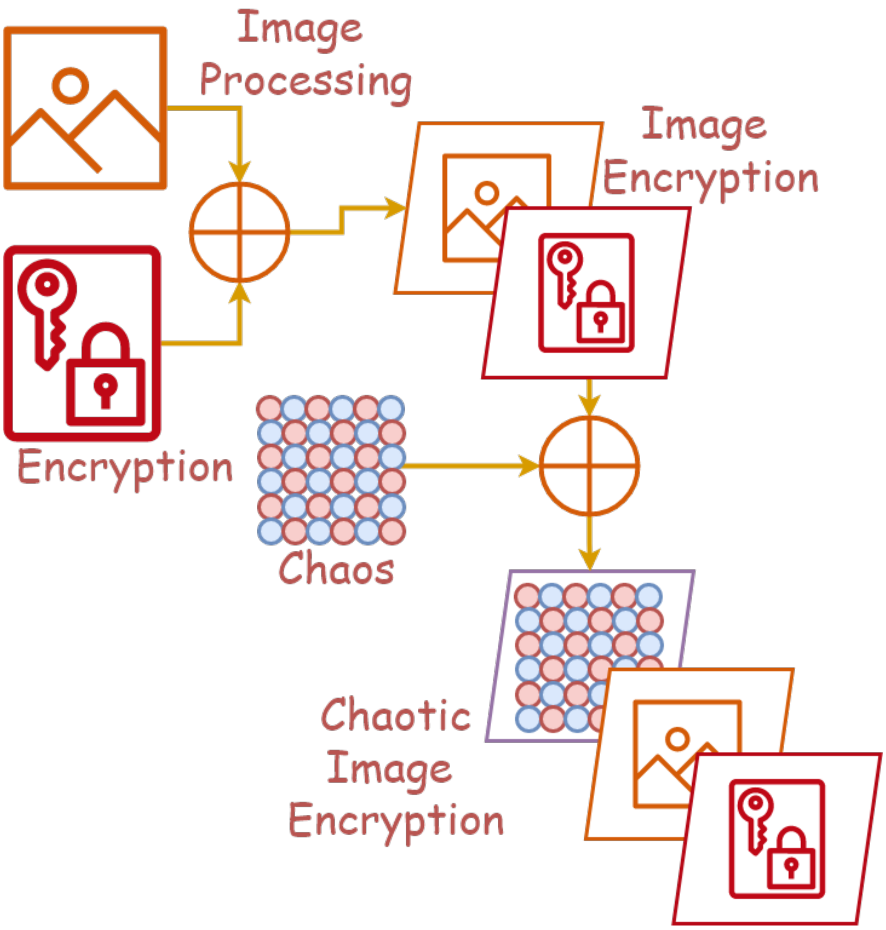

Figure 1. Chaotic Image Encryption: The Convergence Point of Image Encryption and Chaos Theory.

A comprehensive survey on research works focusing on chaotic image encryption can pave the way for further research in this area via highlighting current trends, shedding light on less-studied related topics, and developing directions for future research in this field. In addition to presenting such a survey, this paper establishes an ecosystem for chaotic image encryption. The ecosystem contains the following items.

- **Challenges:** The problems that can potentially make chaotic image encryption difficult, costly, or challenging.
- **Applications:** Environments or areas wherein chaotic image encryption has been demonstrated to be of assistance or efficiency.
- **Enablers:** The technologies or branches of science that can support chaotic image encryption via improving its feasibility, security, performance, or cost efficiency.

The literature comes with several surveys somehow relevant to the work of this paper. However, some of them are too outdated for such a fast-moving research area. Some existing surveys do not focus on chaotic image encryption, and others fail to develop an ecosystem for chaotic image encryption or a future roadmap for further research in this area. These shortcomings motivate our work in this paper.

The rest of this paper is organized as follows. Section 2 studies existing surveys and their shortcomings to highlight our motivations for the work of this paper. Section 3 discusses the state-of-the-art of chaotic image encryption in chaos, image, and encryption aspects. Section 4 studies the ecosystem of chaotic image encryption. Section 5 develops the future roadmap, and lastly, Section 6 concludes the paper.

2. Existing Surveys

As suggested by the topic of this survey, as well as the future predicted in Section 5, relevant surveys focusing on the following topics are deemed relevant:

- Surveys on Image encryption;
- Surveys on chaotic image encryption;
- Surveys on AI-assisted image processing;
- Surveys on AI-assisted image encryption.

In the following, each of the above categories are briefly reviewed. In each category, surveys are studied ordered by their publication year.

2.1. Surveys on Image Encryption

Image files are increasingly distributed across the Internet. This distribution requires security techniques that are different from traditional practices to manage confidentiality. The reason is that images can be vulnerable to several attacks, particularly if these files are sent through insecure channels. Medical images, for example, contain highly sensitive data, and thus, sending these images over the network requires a strong encryption algorithm that protects against these attacks [16].

In recent years, reviewing the literature of image encryption has been of interest to researchers [17,18]. Moreover, different related topics have been reviewed. For example, some researchers have conducted surveys on the techniques for encrypting plaintext into images through an algorithm that calculates the RGB value [19]. Furthermore, some related techniques such as image steganography have been studied along with image encryption [16]. As another topic of interest, some surveys have focused on the applications of image encryption in specific areas [20].

2.2. Surveys on Chaotic Image Encryption

There are some reviews directly focusing on the applications of chaos theory in image encryption. However, some of the surveys studied above (including the one reported in [21]) are too outdated. Moreover, although a few of them develop a future roadmap, all of them fail to establish an ecosystem for chaotic image encryption.

Deepa and Sivamangai [22] argued that a maliciously modified medical image makes it more difficult to diagnose an actual disease. This raises a critical need for the confidentiality of clinical images. On the other hand, the encryption time can pose a heavy overhead on the medical communication and processing systems. They claimed that this tradeoff is best resolved by DNA cryptography and chaotic cryptography. In their review, they reported some qualitative and quantitative measurements extracted from existing relevant research works to show how the tradeoff is resolved by the mentioned technologies. Moreover, they established some guidelines for further research in this area.

Yadav and Chaware [23] believe that despite existing encryption and information hiding techniques, information can be stolen and copyrights can be infringed because of vulnerabilities in available methods. They first presented a review of state-of-the-art image encryption methods. They especially focused on joint encoding (error correction) encryption methods. Then, they proposed a novel method based on Low-Density Parity-Check (LDPC) code and chaotic maps with the support of the Advanced Encryption Standard (AES) and Substitution boxes (S-boxes).

Some existing reviews take a comparative approach. For example, the advantages and disadvantages of existing chaotic image encryption methods were compared in [24]. Another relevant survey was reported in [25], where the authors reviewed and compared some one-dimensional chaotic maps with some hyper-dimensional ones with respect to their applications in image encryption. As another example, the authors of [26] highlighted chaotic encryption as a promising solution for encrypting images and videos, wherein neighboring pixels are highly correlated. They presented a review on existing chaotic methods for image encryption with the goal of identifying the most proper chaotic map.

They studied tent map, logistic map, sine map, etc., and suggested Arnold's cat map as the most promising chaotic map for this purpose. Moreover, in [27], the authors reviewed and compared image encryption methods based on five traditional algorithms, namely Blowfish, RSA, El-Gamal, AES, and DES with some chaos-based methods in terms of performance.

2.3. Surveys on AI-Assisted Image Processing

Reviewing existing AI-assisted image processing methods has been of interest to many researchers. For example, a survey reported in [28] focused on the interactions between machine learning and binocular stereo for depth estimation from images. Depth estimation has many practical purposes in fields such as 3D image reconstruction and autonomous driving. Included in the many techniques for estimating depth, stereo matching compares two images for pixel disparity and utilizes triangulation to determine the depth of the pixel. Data-driven and learning-based techniques have been applied to stereo matchingwith outstanding success, but the reverse has also yielded promising advances in using stereo matchingto develop new methodologies based on deep networks.

Another relevant review studied deep learning-based Multi-Focus Image Fusion (MFIF) methods [29]. MFIF is an image processing technique for fusing multiple images with differing depths of fields to create a single in-focus image. Propositions for solving the MFIF problem using deep learning techniques have been growing at a rapid rate since 2017, although none yet have shown any advantages or performance improvements over traditional methods. The applications of deep learning in image segmentation were studied in another survey [30]. Image segmentation, the process of partitioning an image into two or more segments, has a wide range of use cases in fields such as video surveillance, image compression, augmented reality, and scene interpretation. Algorithms based on deep learning models have demonstrated very impressive results, often outperforming traditional segmentation algorithms on many popular benchmarks.

2.4. Surveys on AI-Assisted Image Encryption

As a branch of AI-assisted image processing, AI-assisted image encryption has received a research focus in recent years. A few researchers have conducted surveys on existing research works in this area. As an example, one may refer to [31], wherein the applications of neural networks in image encryption for optical security in the healthcare sector were studied. Image encryption is an important component in the healthcare sector for improving the security of patient images gathered from sources such as ultrasounds, MRI scans, and X-rays. Neural networks are heavily used to provide security and privacy through encryption, although the algorithms are currently limited by their complexity and speed, and therefore, much research in the field is focused on optimization.

Table 1 summarizes the surveys discussed above in order to highlight their shortcomings, which motivated the work of this paper.

Table 1. Summary of Existing Surveys.

Survey	Year	Chaotic	Ecosystem	Roadmap
[17]	2021	No	No	No
[19]	2020	No	No	No
[32]	2020	No	No	No
[18]	2020	No	No	No
[16]	2018	No	No	No
[20]	2018	No	No	No
[33]	2015	No	No	No
[21]	2014	Yes	No	No

Table 1. *Cont.*

Survey	Year	Chaotic	Ecosystem	Roadmap
[22]	2022	Yes	No	Yes
[23]	2021	Yes	No	No
[24]	2019	Yes	No	No
[25]	2021	Yes	No	Yes
[26]	2021	Yes	No	No
[27]	2017	Yes	No	No
[28]	2021	No	No	No
[29]	2021	No	No	No
[30]	2021	No	No	No
[34]	2020	No	No	No
[31]	2020	No	No	Yes

In Table 1, each entry in the first column contains a survey. The second column states whether or not the survey is focused on chaotic image encryption. The third column demonstrates whether or not the survey establishes an ecosystem for chaotic image encryption. Finally, the fourth column contains "Yes" if the survey develops a future roadmap for the field. It contains "No" otherwise.

3. State-of-the-Art

Research on chaotic image encryption is going on in three aspects; chaos, image, and encryption. These aspects are shown in Figure 2. The state-of-the-art in each of the mentioned aspects is reviewed below.

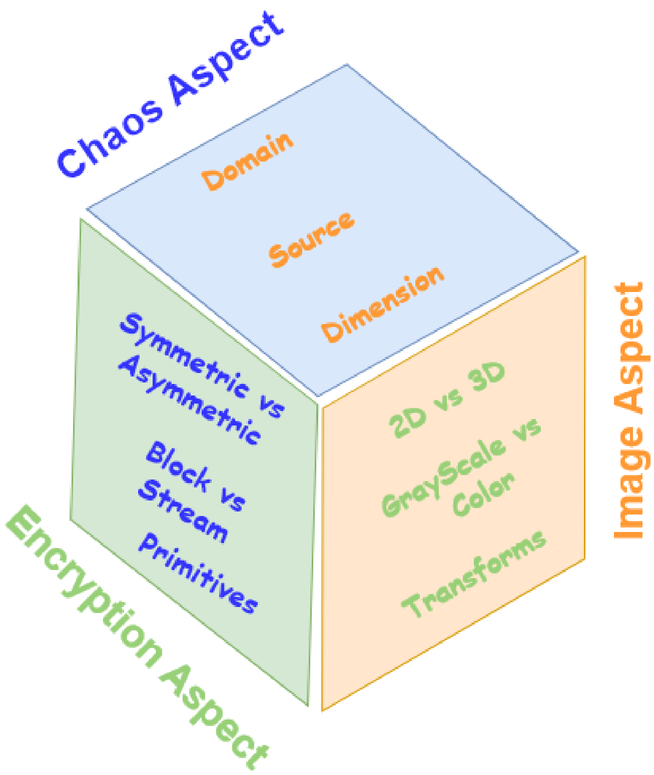

Figure 2. Aspects of Research on Chaotic Image Encryption.

As seen in Figure 2, the chaos aspect is about chaos domains, sources, and dimensions. The image aspect studies 2D versus 3D images, gray-scale versus color images, and image transforms. Moreover, the encryption aspect is related to symmetric versus asymmetric encryption, block ciphers versus stream ciphers, and cryptographic primitives. The research works reviewed in this section are categorized according to these aspects.

3.1. State-of-the-Art in Chaos Aspect

Researchers focusing on the chaos aspect have tried different chaos domains, sources, and dimensions. These concepts are studied below along with related research works.

3.1.1. Chaos Domains

Chaos is studied in three domains; space domain (spatial chaos), time domain (temporal chaos), and space–time domain (spatio-temporal chaos). All of these domains play roles in chaotic image encryption. These roles are reviewed in the following.

Spatial Chaos

Spatial chaotic systems and maps are functions that only depend on an input value to determine the state. They have many uses in image encryption; for example, ShuTang et al. [35] utilized a 2D spatial map in a novel image encryption algorithm that exhibits strong security after applying key sensitivity tests, adjacent pixel correlation analysis, keyspace analysis, and testing against various attacks. Other works in the spatial domain include that performed by Faragallah et al. [36], where they compiled a report investigating the effectiveness of several chaotic maps in the spatial domain, those being the Arnold cat map, baker map, and logistic map. The report describes the analysis of the maps' effectiveness in a novel encryption scheme using visual, entropy, histogram, encryption quality, differential, Known Plain Text (KPA), and Chosen Plain Text (CPT) analysis.

Temporal Chaos

A temporal system only depends on a time index and the state of the system at the previous index to determine the current state. Once such pure temporal chaos system, referred to as a "super-chaotic" map, was utilized by Wang et al. [37] in a proposed image encryption algorithm that exhibited strong security properties such as a large keyspace, high key sensitivity, and statistical analysis resistance.

Spatiotemporal Chaos

A spatiotemporal chaotic system depends on both the spatial domain (input) and the time index. Encryption schemes using spatiotemporal chaos have been proposed by Xin et al. [38] and Luo et al. [39] where the chaos systems were paired with the Discrete Cosine Transform (DCT). The former additionally employs the Propagating Cipher-Block Chaining (PCBC) mode to achieve the image encryption, which contrasts with the work performed by He et al. [40], where the basic Cipher Block Chaining (CBC) mode was opted for instead. All three algorithms exhibit strong security when analyzed using encryption analysis methods.

Another work in the spatiotemporal domain was performed by Xingyuan et al. [41]. In their paper, they proposed a novel spatiotemporal chaos model called the Logistic-Dynamic Coupled Logistic Map Lattice (LDCML). Analysis of the proposed map demonstrated strong chaotic properties, and when applied to image encryption, the further experimental analysis showed high levels of effectiveness.

3.1.2. Chaos Sources

Chaos can be created using mathematical or physical sources. In the following, we discuss the role of both types in the state-of-the-art of chaotic image encryption.

Mathematical Sources

Well-known mathematical chaos sources commonly used for image encryption purposes are studied below:

- Chaotic systems and maps
  These are functions originally designed for creating chaos. Chaotic systems and maps play a critical role in chaotic image encryption. To mention a few, one may refer to the following:
  - Fractional-order chaotic system
    Fractional calculus goes back more than 300 years, with modern studies focusing on systems such as the fractional-order Chen, Lorenz, and Liu systems [42]. A novel switching fractional-order chaos system was proposed by Hou [42] and utilizes controlling switches to switch between its sub-systems and achieve a strong chaos source for applying the exclusive Or (XOR) operation against the plaintext image.
    Another algorithm utilizing fractional-order systems was proposed by Wei [43], which opts to use a more standard third-order fractional system, as well as a novel Josephus scrambling algorithm and circular diffusion to achieve desirable encryption properties and resilience against common attacks.
  - Arnold cat map
    Arnold mapping is a well-know transposition chaotic map that, in the context of cryptography, was used by Ranimol and Gopakumar [44], as well as Zhang et al. [45] to provide a method of permutating and de-correlating adjacent pixels in their proposed encryption algorithms. Both algorithms were proven to exhibit a large keyspace with high key sensitivity and be capable of resisting common attacks such as brute force, entropy, CPT, and KPT.
  - Coupled map lattice
    A Coupled Map Lattice (CML) is a form of spatiotemporal chaos map efficient for random number stream generation. In one use case, Wu [46] proposed a novel implementation of the CML to create encryption streams dependent not only on initial values, but also on intermediate cipher images by using said ciphertexts to modify the CML parameters. This adds a layer of plaintext dependency, which aids in the defense against several attacks.
  - Lorenz map
    A Lorenz system is a type of differential equation that is highly susceptible to initial conditions. Jiang and Fu [47] proposed an image encryption procedure in which the key is composed of the three inputs to a 3D Lorenz system and utilizes the chaotic nature of said system to provide strong security.
  - Logistic map
    A logistic map is a relativity simplistic mathematical mapping function, which when influenced by particular control values, acts chaotically. An algorithm proposed by Sharma and Bhargava [48] utilizes a two-step interactive logistic map, where the next input is dependent on the previous two outputs, as a source of chaos. Similar work was performed by Li-Hong et al. [49], where they used a more standard logistic map and paired it with a hyper-chaos system to improve key generation effectiveness. Likewise, Mu and Lui [50] also found success utilizing the logistic map for key generation.
  - Tent map
    Wu et al. [51] proposed an image encryption algorithm using the CTM, and the rectangular transform was later analyzed by Zhu et al. [52] and improved upon to better protect against plaintext attacks such as CPT and KPT. The Chaotic Tent Map (CTM) is a mapping function that, when configured with control values in a particular range, behaves chaotically.

- Lotka–Volterra
  A Lotka–Volterra chaotic system is a third-order differential equation in a similar family to other systems such as Lorenz, Rossler, Shua, and Chen. In a particular case study by Zahir et al. [53], an encryption procedure was proposed that utilizes the Lotka–Volterra chaotic system to aid in the creation of Substitution boxes (S-boxes) with strong confusion properties. The resulting S-boxes were found to satisfy the five criteria (bijective, non-linearity, strict avalanche, bit independence, input/output XOR distribution) required for acceptable use in cryptographic algorithms.
- Henon map
  The Henon map was first discovered in 1978 and can be described as a 2D mapping function with two control parameters, which, when chosen strategically, enable the map to behave chaotically. Tresor et al. [54] proposed an image encryption algorithm utilizing Henon maps for shuffling the pixels of the image and 4D Qi hyper-chaos to generate keys for encryption. Experimental analysis of the algorithm demonstrates strong cryptographic properties and resistance against common attacks.
- Logistic-sine system
  A Logistic-Sine System (LSS) is a discrete combination of the logistic and sine maps, both of which exhibit chaotic behavior under particular initial conditions. Zeng and Chen [55] referred to such a combination of the two maps as a *compound chaotic map* and utilized it in a novel encryption algorithm using XOR and modulus operations.
  Zhao et al. [56] investigated the inefficiencies with single chaos systems and proposed a novel algorithm utilizing LSS and cascade chaos to improve upon said inefficiencies. Experimental analysis through simulation has proven the new algorithm to be highly resilient
  In another study, Lu et al. [57] conducted cryptanalysis on an existing algorithm based on multiple S-boxes, but were able to break it using CPT attacks. A new algorithm was proposed to improve upon the old one and involved only a single S-box constructed utilizing LSS. Further cryptanalysis of the new algorithm showed improvement over the original and was also quite fast.
  Variants of LSS have also been employed in encryption algorithms, such as a 2D Logistic Modulated Sine Coupling Logistic (LSMCL) map proposed by Zhu et al. [58], a Logistic Sine Modulation Map (LSIMM) proposed by Zhang et al. [59], and a 2D Logistic Adjusted Sine Chaotic Map (LASCM) proposed by Balakrishnan and Mubarak [60]. In all cases, theoretical analysis and simulations determined the algorithms to be both secure and efficient.
- Baker map
  The baker map is a bijective permutation function that operates on an MxM matrix by randomizing its cells according to a secret key and is well respected in the image encryption community. Elshamy et al. [61] utilized the baker map in an image encryption algorithm to improve upon a classic technique known as Double Random Phase Encoding (DRPE). The proposed algorithm uses the map to pre-process the image before applying DRPE, and experimental analysis showed significant increases in security as opposed to using DRPE alone.
  Another algorithm utilizing the baker map was proposed by Tong et al. [62], where high-dimensional dynamical multiple chaos was paired with the baker map to achieve a larger avalanche effect. Experimental results again showed significant increases in security when

- Tinkerbell map
  Krishna [63] proposed an encryption algorithm utilizing Tinkerbell maps, a pair of chaotic functions, to inject strong pseudo-random numbers in multiple points during the encryption and decryption process. Differential and correlational analysis of the algorithm showed the proposed method to be highly efficient.
- Cubic map
  A cubic map is a single-dimensional chaotic function that produces values on the interval [0, 1] and can be controlled by a single mapping parameter. Kavinmozhi et al. [64] proposed an encryption technique that employs a hybrid chaos source composed of the cubic and tent maps, as well as the Iterative Chaotic Map with Infinite Collapses (ICMICs). The resulting hybrid map is used with the XOR operation to achieve encryption, and an analysis of the algorithm showed that it is suitable for repeated use and is resilient against attacks.
- Gingerbreadman map
  Savitri et al. [65] used the Gingerbreadman map, a 2D chaotic map, to generate encrypted keys for use with the well-known Cipher Block Chain (CBC) encryption algorithm. Using the map in this algorithm greatly improves CBC's performance when applied to images, and a visual comparison demonstrated massive improvements.
- Tangent map
  Moysis et al. [66] proposed a Random Number Generation (RNG) algorithm based on the usage of the mathematical hyperbolic tangent function. When the RNG algorithm was applied to image encryption, the resulting procedure demonstrated strong cryptography
- Multiple maps
  Mixing multiple mapping functions in image encryption algorithms can serve multiple purposes. For example, Bisht et al. [67] employed a verity of different maps to achieve tasks such as more chaotic permutation, diffusion, and RNG. A similar technique employing various maps in different stages of the encryption procedure was also proposed by Wang et al. [68].
  Fu et al. [69] proposed a novel keystream generation technique utilizing multiple chaotic maps that incorporates the plaintext itself into the stream. The algorithm was motivated by the need to defend against CPT and KPT attacks, and an analysis of the algorithm showed it is effective in achieving its goal.
  In terms of areas of application, stronger algorithms enforced by the use of multiple chaotic maps are important in numerous fields. For example, Choi et al. [70] proposed an algorithm using multiple maps for encrypting colored medical images, which can be seen as unique in their size and sensitivity. Experimental and statistical analysis of the resulting procedure showed it is secure for use with healthcare images.

• Other mathematical sources
  In addition to chaotic systems and maps, some researchers have used the following mathematical designs, which have not been originally defined for chaos creation:

  - Space-filling curves
    Fractal geometry has several intriguing properties, such as self-similarity, composition by iterative methods, and a complex structure. Zhang et al. [71] utilized Hilbert curves and H-fractals, types of self-filling curves, in a novel image encryption algorithm. This algorithm alternates the use of both curves to efficiently scramble the pixels of the image.
  - Memory cellular automata
    Cellular Automata (CA) can best be described as a grid of cells with a finite set of states and a transition function that governs how cells change state over time. Whereas a standard CA only depends on the generation t-1, Memory Cellular

Automata (MCA) depend on more parameters. When the MCA's rules are defined by chaotic maps, the structure becomes a powerful tool for image encryption. Several algorithms using various-order MCAs have been proposed, for example a 4D MCA by Aslam et al. [72], a 2D MCA by Hibibipour et al. [73], and an indefinite CA by Hibibipour et al. [74].

  - Transcendental numbers
    In mathematics, a transcendental number has the characteristic that digits to the right of the decimal have no pattern [75]. Garcia et al. [75] proposed an image encryption algorithm that uses chaos and the transcendental number Pi, dubbed Chaotic Pi Ciphering (CPC). The algorithm uses Pi and a chaos source created using differential equations to generate cipher keys and substitution boxes.

Physical Sources

In addition to mathematical sources, chaos can be created using physical phenomena and used in chaotic image encryption:

- Optical Chaos
  Our physical world can provide many forms of chaos, with just one example being light. In studies by Xie et al. [76] and Lui et al. [77], they found success in producing a chaotic base for image encryption algorithms using lasers. Extensive security testing of both algorithms showed them to be highly secure and feasible for practical use.
  Other studies have also been carried out, such as those by Li et al. [78] and Liu et al. [79], where optical chaos is utilized for encrypting and then transmitting images for storage in the cloud. Experimental results showed both procedures to be secure and safe for production use.
- Chaotic circuits
  - Chua circuit
    Some physical electronic circuits such as the Chua circuit can produce chaotic behavior. AlMutairi et al. [80] utilized the circuit as a key generator in their proposed image encryption algorithm. By contrast, Lin et al. [81] proposed a similar encryption model, but instead utilized a variant of the classic Chua circuit with a PWL memristor. In both cases, analysis showed the algorithms to exhibit strong security properties.
  - Memristive circuits
    A memristor is a form of electrical component that is capable of exhibiting chaotic behavior. Liu et al. [82] proposed an image encryption algorithm that utilizes 4D memristive hyper-chaos to create chaos matrices. Security analysis showed strong security and cryptographic properties.
    Another image encryption algorithm was proposed by Sun et al. [83] using a memristive chaotic system. The presented system demonstrates a unique property known as multistability, which further improves the chaoticness of the system. Again, security analysis showed the algorithm to possess strong cryptographic properties.
  - Physically Unclonable Functions (PUFs)
    True Random Number Generators (TRNGs), although very important in cryptography, are impossible to achieve in software. To counter this fact, Muhammad et al. [84] proposed an encryption algorithm using a hardware device, a form of physically unclonable function, to generate true random numbers. Through extensive experiments and analysis, the TRNG was successful in passing all tests required for safe use in cryptographic algorithms.

3.1.3. Chaos Dimension

The dimension of a chaos map refers to the number of functions (x(t), y(t), etc.) it is composed of. Many image encryption algorithms utilize chaotic functions of varying dimensions. Chaotic functions used in chaotic image encryption can be categorized as follows:

- One-dimensional
  Work with one-dimensional chaos includes that by Wang and Lui [85], where the novel 1D Sine Chaotic System (1DSCS) was proposed. This system exhibits a large parameter interval as compared to the standard sine map it was built upon.
  Elghandour et al. [86] proposed an image encryption algorithm utilizing the 1D tent map. A similar algorithm also using the tent map was proposed by Tiwari et al. [87]. Extensive testing proved both algorithms to be effective at resisting common cryptographic attacks. The former paper also elaborated on the low chaotic range for the tent map and suggested that future work use a variant with a larger range such as the tent-sine map.
- Two-dimensional
  An image encryption algorithm based on two-dimensional chaos was proposed by Yang and Tong [88]. This algorithm uses the 2D logistic chaotic system and a novel block image encryption procedure. Experimental results demonstrated the algorithm to have strong randomness, low pixel correlations, and high key sensitivity.
- Three-dimensional
  Many image encryption algorithms utilize three-dimensional chaos. One such algorithm was proposed by Qian et al. [89], where they utilized the 3D logistic and cat maps. The novel usage of image reconstruction techniques also improved the effectiveness of the algorithm.
  In an algorithm proposed by Asl et al. [90], the 2D image was converted into three-dimensional space by creating three streams from the red, green, and blue channels of the image. The 3D modular chaotic map was used as the chaos source for encryption.
  Two other algorithms using three-dimensional chaos systems were proposed by Cao and Fu [91] and Xiu-chun and E-Nuo [92], respectively. In the former, the Rossler chaos system was used, whereas the latter study opted to use the Lorenz system.
- Four-dimensional
  Huang et al. [93] proposed a novel four-dimensional chaos system based on concepts known as "shape synchronization" and "driver-response". The complex mathematical underpinnings make the algorithm very difficult to break, and experimental tests in the application of image encryption showed promising results for its effectiveness.
- Five-dimensional
  Zhu and Zhu [94] proposed a novel five-dimensional chaotic map composed of the 2D logistic map and 3D discrete Lorenz map. Experimental simulations of the system when applied to image encryption resulted in high scores in many common encryption strength tests.
- Multiple dimensional
  Work related to mixing maps of varying dimensions in image encryption has also been performed. For example, Qui and Yan [95] proposed an image encryption algorithm using both the 1D logistic map and 3D Lorenz system. Experimental results demonstrated that the algorithm has strong security.
  Parida et al. [96] proposed a novel image encryption and transmission procedure based on Elliptic Curve Cryptography (ECC). Encryption is achieved using 3D and 4D Arnold cat maps as chaos sources, and the Elliptic Curve Diffie–Hellman (EDCH) key exchange algorithm is utilized to establish a shared key between parties. Digital signatures allow the algorithm to authenticate the encrypted message before decryption, and experimental results showed the method to be effective.

3.2. State-of-the-Art in the Image Aspect

The image aspect of chaotic image encryption is about 2D versus 3D, color versus gray-scale, and image transforms. In the following, we discuss each of these topics and show how they are dealt with in research works focusing on chaotic image encryption.

3.2.1. Two-Dimensional versus Three-Dimensional Image

Although 2D images are much more common, 3D images, which can be visualized as 3D meshes, do exist and possess the same encryption requirements as their two-dimensional counterparts. Due to this fact, 3D image encryption algorithms are much less common. However, one such algorithm was proposed by Xu et al. [97].

3.2.2. Gray-Scale versus Color Image

Several algorithms that focus specifically on gray-scale image encryption have been proposed such as one that interestingly utilizes the concept of water waves [98] and another that uses the integer wavelet transform [99]. If color image encryption is required, then gray-scale-specific algorithms will typically not suffice. Algorithms that encrypt color images employ a wide range of techniques such as matrix convolution [100] and 4D memristive hyper-chaos [82]. An approach for encrypting multiple colored images has also been proposed [101], as well as a unique procedure for encrypting and transmitting color images using audio signals [102].

3.2.3. Transforms

Image transforms are of critical importance in chaotic image encryption. Some of them are studied below.

Wavelet

The wavelet transform is a popular method of permutating the cells of a 2D matrix and can yield a significant increase in encryption effectiveness [103]. To fulfill the chaos requirement of good encryption, several chaos sources have been paired with the wavelet transform including an improved 3D cat map [104], a 1D logistic map [105], a 3D logistic map [106], the Arnold map [107,108], and a logistic sequence [108]. Other algorithms utilizing variations of the standard wavelet transform such as the Integer Wavelet Transform (IWT) have also been proposed [109].

Zigzag Transform

The zigzag transform is capable of rearranging the cells of a 2D matrix to heavily decrease the correlation between adjacent pixels, an important property when considering image encryption. Gao et al. [110] proposed an algorithm for image encryption utilizing a more complicated implementation of the transform that yields better security.

Cosine Transform

Zhang et al. [111] proposed an image encryption algorithm utilizing the Discrete Fraction Cosine Transform (DFrCT), which has additional benefits over the standard Discrete Cosine Transform (DCT) that make it more suitable for image encryption.

Contourlet Transform

The contourlet transform provides a method of decorrelating the cells of a 2D matrix and was designed to improve upon the shortcomings of the wavelet transform when dealing with natural images. Jiang et al. [112] proposed an image encryption algorithm utilizing the transform, which has some desirable attack resistances, for example against JPEG compression.

Linear Canonical Transform (LCT)

Li et al. [113] proposed an image encryption algorithm utilizing LCT that is both speedy in execution and also boasts a large keyspace to protect against brute-force attacks.

3.3. State-of-the-Art in the Encryption Aspect

The last aspect of chaotic image encryption is the encryption aspect, which is about symmetric versus asymmetric cryptography, block versus stream ciphers, and cryptographic primitives. The state-of-the-art in this aspect is studied below.

3.3.1. Symmetric versus Asymmetric Cryptography

Symmetric key encryption involves the use of the same key in both encryption and decryption and is common in many algorithms such as the Advanced Encryption Standard (AES). Ashtiyani et al. [114] proposed an image encryption algorithm for encrypting medical images using a chaotic variant of the Simplified Advanced Encryption Standard (S-AES). Asymmetric key encryption involves the use of different (but related) keys for encryption and decryption. Wu et al. [115] proposed an algorithm that utilizes a complex and irreversible function that causes the algorithm to exhibit asymmetric properties.

3.3.2. Block Cipher vs. Stream Cipher

Block and stream ciphers, although common with arbitrary binary encryption, typically fall short when encrypting images. However, when paired with sufficient chaos, they can be used effectively. Some block ciphers used in chaotic image encryption are studied below:

- Blowflish
  Bora et al. [116] proposed a block cipher using the Blowfish algorithm and cross-chaos map. Cryptanalysis results showed strong security.
- Ecliptic Curve Cryptography (ECC)
  Abbas et al. [117] proposed an Ecliptic-Curve (EC)-based algorithm that utilizes pixel-level parallelism for faster encryption speeds. A different proposal by Benssalah and Rhaskali et al. [118] uses ECC combined with the Hill cipher and Arnold cat map to achieve a strong encryption algorithm targeted at medical images.
- El-Gamal
  El-Gamal is a type of EC commonly utilized in cryptography. For example, Luo et al. [119] proposed a public-key-based image encryption algorithm utilizing the El-Gamal EC to address common issues with key management. In another proposal by Yousif et al. [118], El-Gamal was used to encrypt images that were first permutated using zigzag and spiral scanning.
- Rijindal
  Dsouza and Sonawane [120] proposed a novel technique of using images as the key to encrypt/decrypt a directory in a file system. This technique employs both AES and Rijideal ciphers, and evaluation results demonstrated its effectiveness.
- Rivest–Shamir–Adleman Cryptosystem (RSA)
  Nkapkop et al. [121] developed a novel asymmetric image encryption algorithm using RSA to solve the issue of key management. This algorithm uses the RSA key pairs to encrypt the initial values and parameters of the chaotic function so that the public key can encrypt images and only the private key can decrypt.
- Data Encryption Standard (DES)
  Zhang et al. [122] proposed an image encryption algorithm utilizing the logistic chaos sequence for chaotic sequence generation and an improved DES algorithm for encryption. Simulation results demonstrated good security and speed, making it suitable for real-time use.
- Novel block ciphers
  Gupta et al. [123] proposed a novel block cipher using two keys where the image is split into four blocks; each is encrypted n times, and finally, the keys are inverted and the blocks further encrypted m more times. Evaluation through standard tests demonstrated strong cryptographic properties, making the algorithm usable for real-time connections.

Rani and Kumar [124] proposed a novel stream cipher using a modified RC4 algorithm. The algorithm converts the image into three vectors for each color channel and uses the modified RC4 stream algorithm to encrypt them. Another algorithm utilizing the RC4 stream cipher was proposed by Ginting and Dillak [125]. This algorithm uses the logistic map to generate a keystream for encryption. The algorithm is lossless, which was verified by comparing the hash values of the image before encryption and the image after encrypting, then decrypting.

- Hybrid ciphers
  A hybrid approach utilizing both block and stream ciphers was proposed by Goumidi and Hachouf [126]. This algorithm splits the image into two sub-images and encrypts one using the block cipher and the other using the stream ciphers. The encrypted sub-images are then merged back together to form the final image. The use of two different types of ciphers greatly increases the complexity of the algorithm, leading to stronger cryptographic properties.

3.3.3. Primitives

In the following, we examine the role of cryptographic primitives such as scrambling, bit shuffling, hashing, secret sharing, one-time key, permutation, substitution, confusion, and diffusion in chaotic image encryption.

Scrambling

Scrambling is the process of permutating the pixels (or even bits in a pixel) so that the new ordering is unrecognizable from the original. Various methods of scrambling have been employed including Latin rectangle [127], logistic chaotic [128], and spiral [129].

Bit Shuffling

Bit shuffling is another method of permutating the pixels of an image, specifically at the bit level. Krishnamoorthi et al. [130] proposed a method of bit shuffling in the spatial domain using a tent map.

Hashing

Hashing algorithms are special types of functions that take an input of any length and produce an output that is always the same length. The SHA algorithm specifically also has the added bonus of being highly input sensitive, that is to say, small changes in the input create a very different output.

In the context of image encryption, one common use of hash algorithms is to generate the keystream. For example, Bhadke et al. [131] utilized SHA-256 and the Lorenz chaos attractor to generate strong key streams. Slimane et al. [132] also proposed an algorithm using the Lorenz chaos attractor and a hash algorithm, although they opted to use SHA-1 instead.

In a paper by Lui [133], a novel encryption algorithm using SHA-3 and stenography was proposed. This algorithm embeds the hash of the plaintext image into the cipher image using stenography. This makes the algorithm very sensitive to the plain image, which in turn yields stronger security.

Permutation, Substitution, Confusion, and Diffusion

- Permutation and diffusion
  Permutation is the process of rearranging elements in a structure, which, in the context of images, refers to scrambling the pixels. Abd-El-Hafiz et al. [134] performed an evaluation on three different permutation methods (discrete chaos, vectors, and Arnold cat map) and found that discrete performed the best.
  Diffusion is the process of ensuring there is no statistical significance to the resulting structure. In the context of images, this refers to scrambling the pixels of the image to eliminate the correlation between adjacent pixels. Ping et al. [135] proposed a novel

digit-level permeation algorithm that additionally employs a high-speed diffusion algorithm. Evaluation results demonstrated high security and efficiency.
Combining permutation with diffusion into the same stage of encryption aims to combat hackers who try to break each stage separately [136]. Liu et al. [137] proposed an algorithm to perform permutation and diffusion simultaneously. The algorithm additionally uses a Hopfield chaotic neural network to perform further diffusion, which gives the algorithm greater key sensitivity.

- Confusion
Confusion in encryption refers to the level of dependency elements of the cipher-text have with the key. As seen with permutation, confusion is often integrated with diffusion for the same reasons. For example, Run-he et al. [138] proposed an image encryption algorithm that achieves an integration of confusion and diffusion by XORing the plain image with chaotically generated offset matrices.
- Substitution
Substitution involves replacing an element with something else in a predictable and invertible manner. The substitution requirement is commonly implemented using S-boxes, which are matrices that define how each input maps to its substituted value. For image encryption, chaos-based S-boxes include those generated from the chaotic sine map [139] and the logistic map [140]. Wang and Zhang [141] also proposed an algorithm with multiple S-box substitutions, where the order of the boxes is determined by a random chaos sequence. Another algorithm proposed by Khan et al. [142] splits the image into four blocks and applies a different S-box to each block. These S-boxes each originate from a different encryption algorithm (AES, PQL, APL, and Shipjack). Another paper by Lidong et al. [143] proposes a dynamic encryption algorithm so that the cipher image is always different even if the same key and plain image are used.

One-Time Key

Rehman et al. [144] proposed an image encryption algorithm that uses a one-time-key to generate chaotic maps using the hash of the plaintext image. The algorithm employs a novel concept known as a rotor machine, and through simulation, the results showed that the algorithm possesses strong cryptographic properties.

Secret Sharing

Multiple Secret Sharing (MSS) in the context of image encryption is where k plaintext images are required to create k cipher-text images, and those same k cipher-text images are required to obtain even just one plaintext image [145]. Guo et al. [145] proposed an MSS algorithm for images that addresses common shortcomings.

4. Ecosystem

In this section, we try to establish an ecosystem for chaotic image encryption. To this end, we try to highlight challenges, application areas, and enabling technologies.

4.1. Challenges

The main challenges faced by researchers focusing on chaotic image encryption include encrypted image processing, attack protection, and evaluation. These challenges are studied below.

4.1.1. Encrypted Image Processing

Processing encrypted images is a highly challenging job. The related challenges are discussed in the following.

Data Hiding

Data hiding refers to the technique of hiding information in an encrypted image without knowledge of the original contents [146]. One common method of Reversible Data

Hiding in Encrypted Images (RDHEIs) is Block Permutation and Co-Modulation (BPCM); however, Wang et al. [147], through cryptanalysis, determined that the method cannot protect against KPAs.

Another big challenge with current data hiding methods is capacity limits. A high-capacity alternative utilizing a blockwise multi-predictor and Huffman coding was proposed by Zhang et al. [146]. Other capacities improving techniques based on pixel correlation preservation [148] have also been proposed.

Other novel contributions to data hiding have been proposed. Xiong et al. [149] proposed improvements to common techniques to increase the resistance against common attacks such as JPEG compression and noise addition. Wang et al. [150] proposed a novel method of decryption using separate keys for both the decryption of the image and the reversion of the data hiding.

Image Retrieval

The image retrieval problem refers to the issue of maintaining privacy when outsourcing image search services in the cloud. Work by Huang et al. [151] aimed to fix issues with low accuracy and high involvement from image owners using the process of extracting image features using neural networks and encrypting using the k-Nearest Neighbors (kNN) algorithm. Other progress in the field includes work involving multi-owner access by Tong et al. [152].

Image Compression

Techniques of mixing image encryption with lossy compression have been proposed. One such proposal was made by Zhang [153], where an iterative reconstruction technique was utilized for decompression. However, the encryption technique used was relatively weak compared to exiting algorithms.

Another algorithm was proposed by Qin et al. [154], where a selective compression technique is paired with inpainting, a method of restoring missing pixels, to reconstruct the image.

Image Folding

A novel procedure known as encrypted image folding was proposed by Bowley and Rebollo-Neira [155]. This technique not only encrypts the image in question, but also decreases its dimensionality, allowing for more efficient storage.

4.1.2. Attack Protection

There are several attacks that can be conducted against chaotic image encryption. Research works focusing on these attacks are studied below.

Plaintext-Related Image Encryption (Protection against Plaintext Attacks)

Good encryption algorithms should possess resistance to common types of attacks including plaintext attacks. Many resilient algorithms have been proposed such as the one by Khan et al. [156], where they used a random DNA sequence to initialize chaos maps. Niu and Zhang [157] proposed another resilient algorithm utilizing pixel permutation and Josephus traversing. Yet another algorithm based on Chen's chaotic system was proposed by Fu et al. [158], aiming at improving resilience against known/chosen plaintext attacks. In the diffusion stage of this algorithm, the key stream elements created by Chen's chaotic system are rotated in such a way that the rotation is dependent on the value of the plain pixel. This way, the key stream is a function not only of the key, but also of the plain image. This notably strengthens the cryptosystem against known/chosen plaintext attack. Critiques based on the attack resilience of existing proposed algorithms have also been made. One such critique was made by Liu et al. [159], where vulnerabilities related to diffusion and permutation in a hyper-chaos algorithm were discovered and improved upon.

4.1.3. Evaluation

Many researchers are interested on the evaluation of chaotic image encryption methods. The evaluation process may include attack, cryptanalysis, or benchmarking. These evaluation approaches are discussed in the following.

Attack

Yan-Qing and Zhuo-Min [160] performed an analysis of the HYPER-HIE image encryption algorithm based on hyper-chaos. Their analysis attempted to exploit the algorithm's weaknesses in its permutation and diffusion techniques, and their research concluded that the algorithm could not resist chosen plaintext attacks.

Cryptanalysis

The cryptanalysis of many existing algorithms has been performed. One such analysis was performed by Feng and He [161], where an algorithm based on hyper-chaos and DNA failed to account for chosen plaintext attacks. To this extent, the authors of the paper were able to design an attack that reveals the plain image with no knowledge of the key. Another analysis was performed by Liu et al. [162], where an image encryption scheme combining bit-plane extraction with multiple chaotic maps (IESBC) was found to be vulnerable to chosen and known plaintext attacks. The algorithm was then improved upon to score highly with various cryptographic metrics.

Some algorithms also claim to have secure properties, but may fall short. One example is a chaotic Image Encryption Algorithm based on Information Entropy (IEAIE), which was analyzed by Li et al. [163]. This algorithm was found to possess many pitfalls and questionable security metrics. Another example is a color image encryption scheme based on a hybrid hyper-chaotic system and cellular automata analyzed by Li et al. [164]. This algorithm possesses several security drawbacks despite claiming to resist applicable attacks. A more general study of issues with algorithms based on cryptanalysis-driven design were outlined by Muhammed et al. [165].

Benchmarking

Hraoui et al. [166] performed benchmarking on the AES encryption algorithm and another algorithm based on the logistic map. Their results demonstrated that the AES exhibits better security performance, but is computationally slower. The logistic map, on the other hand, is less secure due to a few specific vulnerabilities, but is faster and simpler to implement, making it more ideal for real-time communications.

4.2. Application Areas

As suggested by existing research works, chaotic image encryption is mainly applied to IoT systems, medical systems, and satellite systems. In the following, we study these application areas.

4.2.1. IoT

Image encryption is a necessary requirement in many modern IoT systems, yet the requirements of said algorithms are very steep and their efficiency must be proven. One such algorithm proposed by Nath et al. [167] was simulated in MATLAB and contrasted against existing algorithms to prove its efficiency.

Another novel algorithm was proposed by Boutros et al. [168], where hardware acceleration was used to meet the speed requirements of real-time IoT applications. For a 512×512 image, the algorithm achieved a maximum frequency of 135 MHz and 256 fps.

4.2.2. Medical Systems

Protecting medical records (including images) is not just a privacy concern, but a legal requirement [169]. This is especially true when transferring said medical images over open or public networks [170,171].

Many chaos-based approaches for encryption have been proposed. These approaches often involve chaos maps [169], especially the Arnold cat map [172] and logistic map [171]. Approaches using DNA-based algorithms have also been proposed [173], including a rather novel one by Kumari and Nagaraju [171], where chaotic maps were used to decrease the computational complexity of DNA-rule-based sequences.

The use of key streams is also a common technique. Vaseghi et al. [174] proposed a method for synchronizing chaotic systems at both the transmission and receiver ends so that keys can be obtained from the streams and no keys need to be directly shared. Another novel proposal was given by Han et al. [175], where a logistic map was used to generate a sequence from which a Hermite neural network was trained. This trained network was then used to generate key streams for use in encryption.

4.2.3. Satellite Systems

Transmission of image data over satellite connection poses a unique problem of a non-negligible time delay between the involved parties. A novel solution to this issue was proposed by Vaseghi et al. [176], where Lyapunov stability theory was applied to achieve time synchronization in finite time.

Another algorithm dealing with satellite transmission was proposed by Ibrahim et al. [177], where a new Cascade Modular Tent Logistic Map (CMTLM) was used. Simulation results demonstrated high effectiveness for the algorithm to perform in the satellite cryptosystem.

4.3. Enabling Technologies

In this subsection, we examine the technologies that support chaotic image encryption.

4.3.1. DNA Computing

DNA, formally known as Deoxyribonucleic Acid, is the biological substance that forms our genetic code. DNA can be broken down into four pieces known as ATCG, or formally Adenine, Thymine, Cytosine, and Guanine [178]. This concept can be used in encryption by encoding the data using this structure and leveraging existing DNA technology and sequences to manipulate it [179]. This encoding scheme has many advantages such as immense keyspace [180], high storage space for data [181], and high parallelism for algorithms [182].

The most common way to implement DNA concepts in image encryption is to pair it with a chaos source that aids in choosing random DNA coding rules or sequences [179]. Many algorithms with varying sources of chaos have been proposed. These include the logistic map [183–186], sine chaotic map [182], sine-Henon alteration map [185], cellular automata [187], optical chaos [188], etc.

The encryption algorithms themselves also employ a wide range techniques. These include encryption then transmission [188], using DNA sequences as a one-time pad [184], the Vigenere cipher [189], matrix subdivision [186], splitting color streams [190], the use of the Chinese remainder theorem [191], and the use of reconfigurable hardware called FPGA.

Several more unique approaches have also been proposed. One such proposal was by Hao et al. [178], where DNA mutations were implemented to improve the randomness of DNA algorithms. A different approach by Gasimov and Mammadov [192] utilizes DNA pseudo-symbols where the standard DNA sequence of four characters (ATCG) is expanded to use eight pseudo-symbols.

A particularly interesting proposal was also made by Iqbal et al. [193], where the concept of the castle piece from the game Chess (also called the rook) was used. These authors argued that simply mixing chaos and DNA is not enough, and to more effectively scramble and confuse the pixels of the image, random movements of the castle piece were simulated on a chessboard with dimensions equivalent to the image.

Statistical and security analyses of several algorithms based on DNA encoding and chaos have been performed; one examples is Özkaynak et al. [194]. In this study, it was found that existing algorithms are vulnerable, and choosing the plaintext strategically can reveal some or all secret parameters. Another research proposal by Ahgue et al. [181] takes a graphical approach to analyzing the security of algorithms. The provided GUI allows for configuring the secret key, encrypting a chosen image, and viewing the statistical analysis.

4.3.2. Quantum Computing

Xu et al. [195] proposed a novel image encryption algorithm involving a quantum chaos map by applying quantum correlation theory to the classic logistic map. The resulting map exhibits strong chaotic behavior and is used to generate chaotic streams for permuting the pixels of the image in question.

4.3.3. Signal Processing

Some signal processing methods such as compressive sensing and differential evolution have played roles in research on chaotic image encryption. These methods and their roles are investigated below.

Compressive (Compression) Sensing

Image encryption algorithms based on compressive sensing theory have been proposed. One such proposal is by Shao et al. [196], where a unique source of chaos from *hybrid analog–digital electro-optic* sources was used. Another proposal was by Zhu et al. [197], where Gauss random matrices were used for compression. Both algorithms exhibited strong cryptographic strength through simulations and experimental analysis.

Differential Evolution

An image encryption algorithm utilizing differential evolution was proposed by Toktas et al. [198]. The differential equation utilizes an algorithm based on natural evolution to find optimal decision variables to seed the [198] chaotic map optimization for image encryption using the triple objective differential evolution algorithm.

4.3.4. Hardware Technology

Many chaotic systems can be very expensive and slow to compute, making them infeasible for real-time scenarios. By comparison, hardware-based approaches are much faster and still maintain the high level of security required [199].

In a proposal by Paliwal et al. [200], chaos generators were implemented in part by the Coordinate Rotational Digital Computer (CORDIC), a hardware-efficient algorithm for calculating various functions such as tangents and hyperbolics. The types of chaos generators used in hardware algorithms are much the same as standard software approaches, such as iterative maps [199], cat maps [201], and the double-humped logistic map [202].

These algorithms are often tested on physical hardware to prove their claimed effectiveness. Examples of the hardware used are the Virtex-IV [203] and the Virtex-5 FPGA [202]. These tests resulted in high throughput with a small utilized area. Zhang et al. [201] also proposed a more generic hardware structure for an algorithm that exhibits good reusability for use in different systems.

4.3.5. Parallel Processing

Parallel processing sees much use in image encryption. In one such proposal by Gu et al. [204], the problem of implementing image encryption in green IoT environments was tackled. The paper discussed the primary concerns, those being limited computing power and long lifetime. These issues were addressed by proposing a novel parallel encryption technique using various chaos maps implemented in a parallel structure.

In another proposal by Fu et al. [205], a novel encryption algorithm was proposed. Said algorithm decomposed the image into eight subplanes and processed each in parallel. Experimental analysis demonstrated that the algorithm possesses high security and runs five-times faster than an equivalent serial method.

4.3.6. Fuzzy Systems

A fuzzy system is based on fuzzy logic, that is values are real numbers between 0 and 1 as opposed to exactly 0 or exactly 1. In a proposal by Mohamed et al. [206], the Choquet Fuzzy Integral (CFI) was utilized to construct better substitution boxes than standard cryptographic methods.

Figure 3 illustrates the established ecosystem.

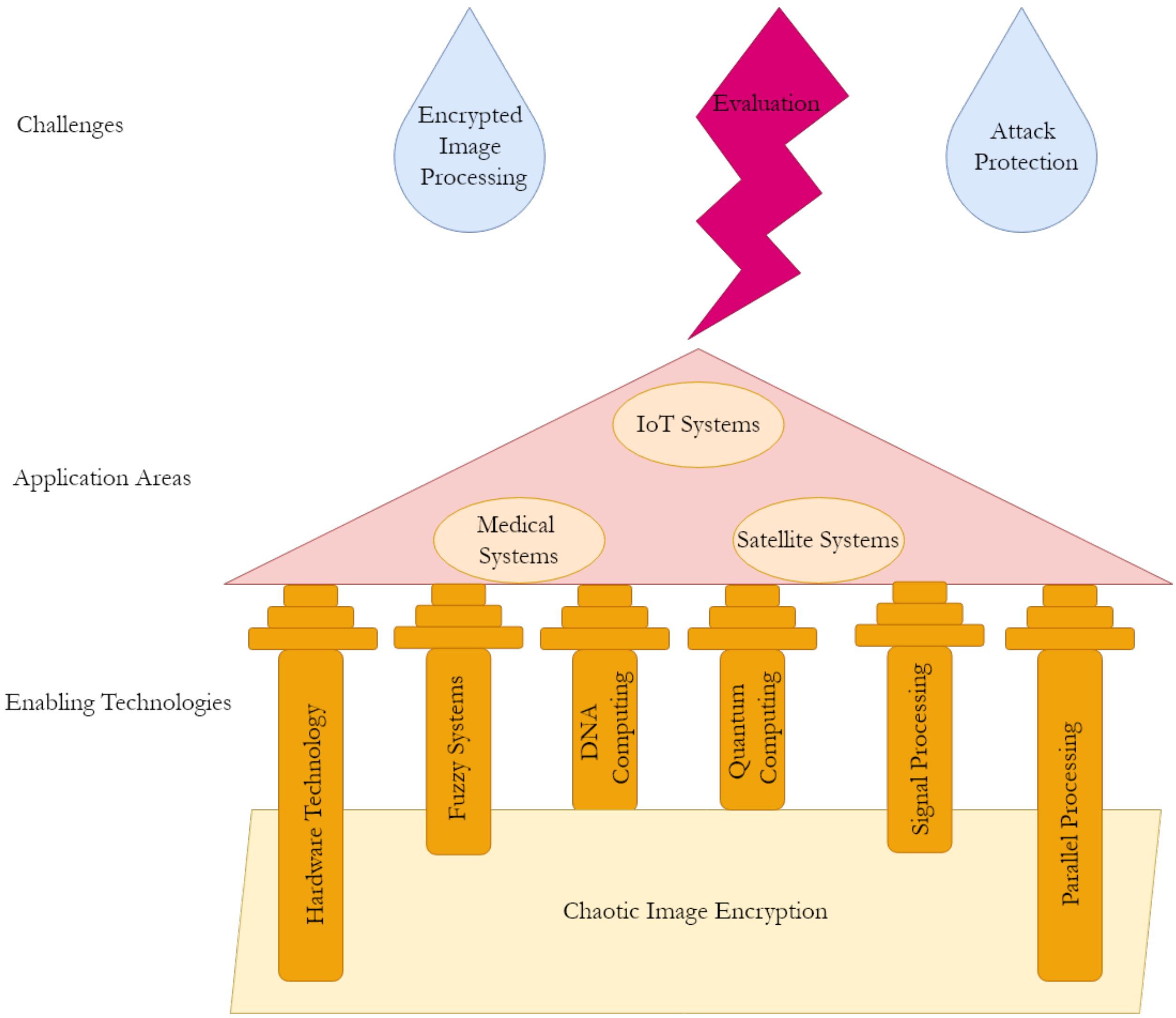

Figure 3. The Ecosystem of Chaotic Image Encryption.

In Figure 3, columns represent enabling technologies. The blocks in the roof denote application areas. Lastly, the rain drops and the thunder represent challenges.

5. Future Roadmap: The Promise of AI

We anticipate that research on chaotic image encryption will move towards quantum-inspired and bio-inspired neural chaotic image encryption in the near future. Our reason for such an anticipation is the existence of the trends discussed in Sections 5.2–5.11.

5.1. Neural Networks in Chaos: Chaotic Neural Networks and Their Applications

The use of chaotic neural networks is wide in application. For example, to solve the problem of degrading performance in Code Division Multiple Access (CDMA) systems due to system capacity and multiple access interferences, Wang et al. [207,208] used a CNN to detect multiple users, a task that is NP-complete. Experimental results demonstrated superior performance to the existing Hopfield-Neural-Network (HNN)-based detector. CDMA is a communication technique where multiple transmitters can send signals simultaneously over a single channel.

CNNs can even be applied on a hardware level. For example, Cao et al. [209] used a novel Chaotic Hopfield Neural Network (CHNN) to optimize the SF6 circuit breaker. Work by Zhang et al. [210] used CNNs to solve a hysteresis bottleneck for the usage of the Magnetic Shape Memory Alloy (MSMA) smart material with promising properties for use in micro-positioning applications.

5.2. Neural Networks in Image Processing

Convolutional Neural Networks (CNNs) see much use in the realm of image processing. Many complex image problems are solved using CNNs, including facade parsing (determining distinct faces of buildings) from street-level images [211], crowd stability calculations (count and density) from video surveillance [212], Hyperspectral Image (HSI) classification [213,214], Polarimetric Synthetic Aperture Radar (PolSAR) image classification [215], medical image diagnostics [216], and tree species identification from aerial images [217].

Another effective use for image processing is to convert data into images so that existing image processing techniques can be used to solve other problems. For example, a technique proposed by Song et al. [218] converts EGG data into images to convert the problem of EGG emotion reading to the problem of image recognition. In another proposal by Lu et al. [219], graph classification using CNNs was mixed with image segmentation to yield better structural information.

CNNs also present several shortcomings when used with image processing. A common issue is the complexity of the networks, which leads to high computational costs and infeasibility for real-time applications [214,215]. The lack of a labeled training table can also be a common issue and leads to over-fitting and loss of detail [213]. To overcome these issues, Fernandes and Yen [216] proposed an algorithm that uses a deepening then pruning approach to shrink the size of a network while maintaining its effeteness. Another proposal by Mei et al. [214] trims the input to the network to use integer values instead of floating point values, which greatly speeds up the computation time.

5.3. Neural Networks in Encryption: Neural Cryptography

Neural cryptography is a recent research trend. Different kinds of neural networks have been used for this purpose [9,220]. Moreover, different cryptographic algorithms have been examined in this area [221]. More importantly, different enabling technologies are used to support neural cryptography. For example, hardware technology can be utilized to embed cryptographic algorithms into neural network accelerators [220].

5.4. Neural Networks in Image Security

Deep-Neural-Network (DNN) and CNN-based image processing have many applications in security, one of the most common being computer vision [222]. Examples include facial and body detection [222], detecting threats (specifically explosives) in X-ray images of passenger baggage [223], and detecting man-made items in millimeter wave images.

Neural networks also see much use in improving the security of image encryption algorithms. In a proposal by Seethalakshmi et al. [224], steganography techniques were improved by splitting the source image into n shares and using neural networks to determine where in the destination image to hide the shares to maximize its security. In another proposal by Sirichotedumrong et al. [225], a privacy-preserving DNN was developed. This DNN takes specially encrypted images as the input so that it can still extract the required features without being able to see the plain image. Furthermore, the testing and training phases for the model can use different encryption keys for further privacy.

In another proposal by Ito et al. [226], a DNN was trained on plain images to transform them into visually secure images. Through analysis, the network was shown to be resistant to inverse transformation attacks where DNNs were trained to invert the transformation. In a different study by Sirichotedumrong et al. [227], this same inverse transformation attack was performed against many existing DNN-based encryption algorithms. It was found that if the images were encrypted using use different keys, then the encryption was secure. If the same key was used for different images, then the data were able to be retrieved.

CNNs can even be used to determine the security of already encrypted images. In a paper by Fezza et al. [228], a CNN was developed to rate an encrypted image based on visual security and visual quality. Su et al. [31] also examined existing algorithms to determine their security. In their study, 30 state-of-the-art image encryption algorithms using neural networks were examined to determine the optimal algorithm.

5.5. Neural Networks in Image Encryption

Neural networks are widely used in image encryption. Different aspects of this trend are explained below.

5.5.1. Network Types

- Back propagation:
  Yang et al. [229] proposed a Backpropagation (BP)-based neural network utilizing fractional-order memristive hyper-chaos to encrypt images. Another proposal by Ismail et al. [230] uses a similar network to encrypt large satellite images. This algorithm is unique in that it is not affected by geometrical image distortions such as translation, size, and rotation.
- Bidirectional:
  Memristive bidirectional associative memory neural networks have been applied to image encryption in proposals by Wang et al. [231] and Xiao et al. [232]. Simulations and experimental analysis demonstrated both algorithms to be highly secure and resist common attacks.
  Several image encryption schemes utilizing cellular neural networks have been proposed. These include one by Zhou [233] using parallel computing, one by Lin et al. [234] using compressive sensing to achieve encryption and compression, and one by Liu et al. [235] using a fractional-order quantum variant of the network. Lin et al. [236] also proposed an algorithm that uses the network to generate a chaotic stream, which is further used to power Latin squares.
  Another proposal by Hu et al. [237] implemented an encryption/decryption scheme using cellular neural networks that can decrypt the image even if parts of it were corrupted in transmission. A similar technique was used by Liu et al. [238], where noise removal was performed on a transmitted image using the special Cohen–Grossberg neural network. Noise removal is key, otherwise the decryption will not work correctly due to the avalanche property of encryption algorithms.

5.5.2. Encryption

Neural networks see much use in image encryption. Kumar and Rohit [239] proposed a novel Wavelet-based Chaotic Neural Network (WCNN) used for image encryption. A different proposal by Joshi et al. [240] also uses neural networks for encryption, but additionally adds impurities to confuse analysts. Other utilized techniques include multi-layer [241] and multi-image [242].

5.5.3. Steganography

Steganography is very similar to encryption, although the goal of steganography is to hide data so that it is not clear any data are even hidden. Preethi and Asokan [243] proposed a technique using neural networks to determine the Regions Of Non-Interest (RONI) in an image that are optimal for implanting a watermark. In a similar proposal by Duan et al. [221], the discrete cosine transform and ECC were used to encrypt the image first and then the well-known SegNet neural network to improve hiding.

5.5.4. Privacy

Maintaining the privacy of images that are processed by AI algorithms is a novel, but important concept. In a proposal by Sirichotedumrong et al. [244], a special privacy-preserving encryption algorithm was used that encrypts the image, but maintains its features, so that a DNN can still read them. In a different paper by Sirichotedumrong et al. [244], this algorithm was tested on the well-known ResNet-18 network.

5.5.5. Synchronization

Work on the synchronization of neural networks is plentiful. Researched techniques include Periodic Self-Triggered Impulsive (PSTI) control [245], neural activation function [246], and unbounded delay.

The types of neural networks involved in synchronization research are also various. These include arrays of coupled jumping delayed neural networks [247], reaction–diffusion neural networks with mixed delays [248], and chaotic memristive multidirectional associative memory neural networks [249].

5.6. Neural Networks in Chaotic Encryption

Thoms et al. [250] proposed an encryption algorithm using key-controlled neural networks, where key generation is based on the chaotic Lorenz system. The algorithm is designed for digital traffic encryption, and cryptographic analysis demonstrated that it performs on par with or better than existing algorithms.

5.7. Neural Networks in Chaotic Image Encryption

A common use for neural networks in chaotic image encryption is to generate the key streams. This can be seen in a proposal by Han et al. [175], where a Hermite chaotic network was trained from a logistic map, and in a proposal by Fang et al. [251].

In a different proposal by Qingmei and Guodong [252], the hyperchaotic properties of cellular neural networks were leveraged to achieve chaotic image encryption. Simulation results in MATLAB demonstrated strong cryptographic properties.

5.8. Neural-like Image Encryption

Zhang et al. [253] proposed an image encryption algorithm using a neuron-like scheme. The image information is used to adjust neuron weightings to achieve effective pixel diffusion. Simulation results demonstrated strong cryptographic properties.

Combinatorial Optimization Problems

Many important problems in computing such as the shortest path, the Traveling Salesman Problem (TSP), Cellular Channel Assignment (CCA), or more generally, sequencing and resource allocation problems have very inefficient exhaustive search solutions [254]. To find the optimal solution, neural networks have been utilized. Some examples are given below.

In a proposal by Shiyu and Jianying [255], a CNN was used to optimize the shortest path problem. In this proposal, a novel post-processing technique was utilized to achieve the optimal solution with high probability. In a different proposal, Zhao et al. [256] used a CNN with the novel ability to characterize local features to solve the TSP with a higher-than-average success rate for obtaining the optimal solution.

Work on optimizing CCA was conducted by He et al. [257] and Zhao and Gan [258], where noisy CNNs and transient CNNs were utilized, respectively. A related problem to CCA is the more general broadcast scheduling problem. Work by Sun et al. [259,260] proposed a novel noise-tuning-based Hysteretic Noisy Chaotic Neural Network (NHNCNN) that optimizes the problem by obtaining the minimum frame length and maximal channel usage. Their work was completed for both wireless multihop networks and pocket radio networks.

The same CNNs can also be used to solve multiple types of optimization problems. For instance, Wang et al. [261] combined the best parts of the existing Chaotic Simulated Annealing (CSA) and Stochastic Simulated Annealing (SSA) techniques to optimize multiple combinatorial problems such as the TSP and CCA. To compare and contrast the many different CNN approaches for solving these problems, Kwok and Smith [262] developed a framework.

5.9. Chaotic Neural Networks in Image Encryption

The application of chaotic neural networks has been of interest to the research community in recent years [263,264]. Different types of neural networks including the Once Forward-Long Short-Term Memory Structure (OF-LSTMS) [265], Hopefield neural networks [266], and cellular neural networks [267] have been used in this area. Moreover different chaotic maps [267] and sequences [265] have been examined in research in this area.

Wang et al. [249] proposed a novel chaotic neural network called a Multidirectional Associative Memory Neural Network (MAMNN). An image encryption algorithm utilizing the network was also designed to demonstrate its chaotic capabilities. In a different paper by Han et al. [175], they proposed an image encryption algorithm based on the Hermite chaotic neural network. This algorithm is targeted for use on medical images, and statistical analysis demonstrated strong cryptographic properties and resilience against common attacks.

5.10. Quantum-Inspired AI

Quantum-inspired Reinforcement Learning (QiRL) is a heavily researched application of quantum theory. It is inspired by the collapse phenomenon and amplitude amplification properties of quantum computing [268]. Li et al. [268] used QiRL to optimize the uplink transmission rate to an Unmanned Aerial Vehicle (UAV) with little context about the clients' geographical location. Another proposal by Dong et al. [269] used QiRL to control the navigation of autonomous mobile robots. Simulation results of the system demonstrated good results as compared to other models.

Another proposal for use of quantum concepts in reinforcement learning comes from Wei et al. [270]. In this proposal, quantum concepts were used to adaptively choose experiences from the replay buffer in reinforcement learning models according to the complexity and the replayed times of each experience. This effectively achieves a balance between exploration and exploitation.

Quantum concepts also see much use in neural networks. Masuyama et al. [271] proposed Quantum-inspired Multidirectional Associative Memory (QMAM). This model allows the neural network to progressively develop a resonance state, from inputs to outputs. In another proposal by Patel et al. [272], a Quantum-inspired Fuzzy-based Neural Network (Q-FNN) was introduced. Quantum computing concepts were used to adjust the fuzzy parameter to optimize the network. Testing on 15 benchmark datasets demonstrated superior results.

5.11. Bio-Inspired AI

Bio-inspired learning is implemented in a wide range of fields, with a common one being computer vision. Yuan et al. [273] proposed a bio-inspired system for Visual Attention Prediction (VAP) by leveraging both low-level contrast and high-level semantic features. Another proposal in the computer vision realm was made by Xu et al. [274], where a combination of neural networks and collected eye-tracking data was utilized to determine if and why a face is perceived as beautiful. Extensive tests on this method using popular datasets demonstrated superior performance.

Reinforcement learning can also see great improvements by pairing it with bio-inspired techniques. For example, Lehnert et al. [275] proposed an autonomous navigation algorithm using visual sensors and auxiliary tasks to balance out the common problem of sparse rewards in standard reinforcement learning. Another proposal by Tu et al. [276] used reinforcement learning to control a mobile hummingbird robot to perform biological-based maneuvers such as rapid escapes and tight body flips.

Bio-inspired learning can even see use in the IoT space. Yang et al. [277] proposed a system for optimizing IoT services to reduce service time and energy consumption inspired by the cooperative nature of the various systems in a biological organism. Gibson et al. [278] also performed work with spam email detection with standard classification models.

Since AI techniques can often be very technical and confusing to newcomers, Duan et al. [279] developed an interactive learning environment for bio-inspired AI called BOLE. This system works with unmanned aerial vehicle paths.

Figure 4 demonstrates how current trends predict future trends. In the left column, icons are joined to form new icons for current trends. In the right column, different icons are joined in a similar vein to create predicted future trends. Arrows join the two columns to show how current trends predict future ones.

The trends in Figure 4 form the following two main lines:

1. The significant role of neural networks in the current state of chaotic image encryption. This role is highlighted by the role of neural networks in the three aspects of chaotic image encryption, namely *chaos*, *image*, and *encryption*.
   The role of neural networks in the creation and exploitation of chaos is studied in Section 5.1. Section 5.2 discusses the role of neural networks in image processing. Furthermore, the role of neural computing in encryption is highlighted in Section 5.3. The next few subsections investigate how neural networks appear in the intersections of these aspects.
2. The significant impact of quantum technology and biological inspirations on the future of neural networks.
   Sections 5.10 and 5.11 discuss the impact of quantum technology and biotechnology on the future of AI, and especially neural networks.

The above two lines clearly will converge at bio-inspired/quantum-inspired neural chaotic image encryption.

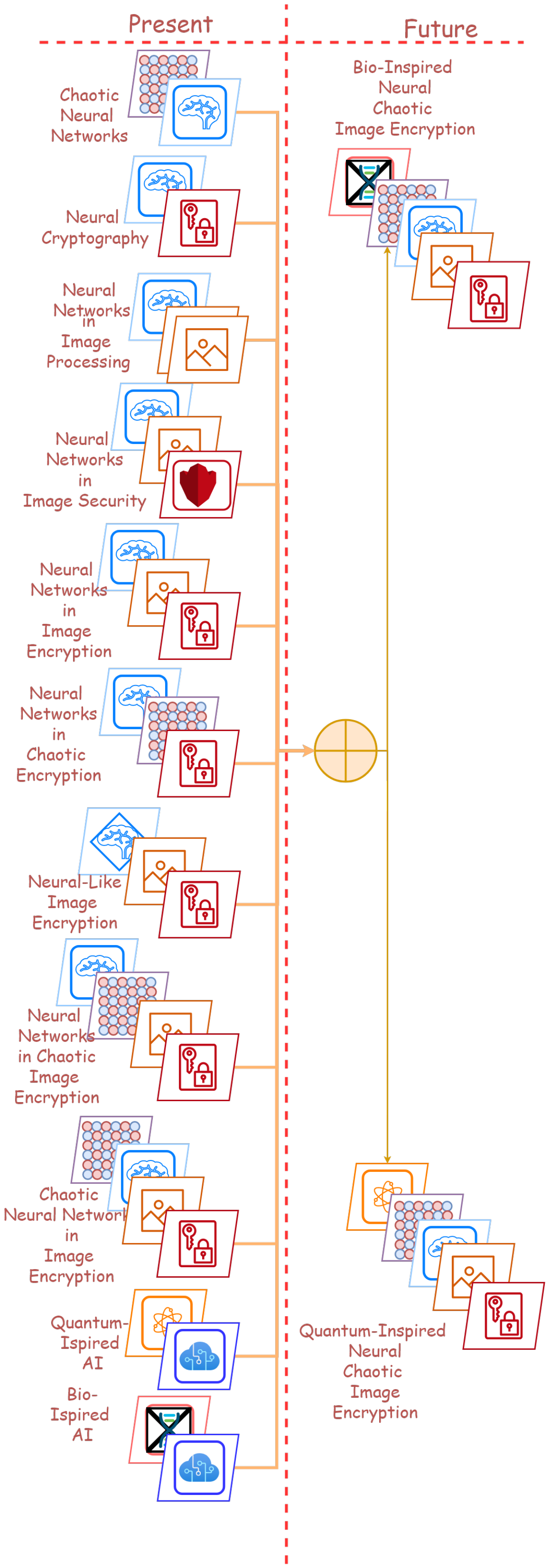

Figure 4. Chaotic Image Encryption Trends (Present and Future).

6. Conclusions

This paper presented of a comprehensive survey of existing work on chaotic image encryption and established an ecosystem, as well as a future roadmap for the field. We identified the challenges of the chaos aspect, the image aspect, and the encryption aspect of this research area. The choices among different chaos domains, sources, and dimensions, as well as the choice between block and stream ciphers or symmetric and asymmetric cryptography are some of these challenges. The work of this survey will help build a strong foundation from which further research can be built. While current research trends indicate a focus on AI and neural networks (chaotic neural networks, chaotic neural image encryption, etc.), predicted trends lean towards quantum and bio-inspired AI (bio-inspired and quantum-inspired neural chaotic encryption). Further research can be performed to expand the ecosystem of chaotic image encryption as these new trends produce more novel results.

Author Contributions: T.K. has contributed to the review. B.Z. has contributed in review, writing and preparation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Preishuber, M.; Hütter, T.; Katzenbeisser, S.; Uhl, A. Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2137–2150. [CrossRef]
2. Lin, C.; Pham, D.; Huynh, T. Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by tsk fuzzy brain emotional learning controllers. *IEEE Trans. Cybern.* **2021**, 1–15. doi: 10.1109/TCYB.2021.3134245. [CrossRef] [PubMed]
3. Liu, S.; Li, C.; Hu, Q. Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE Multimed.* **2022**, *29*, 74–84. [CrossRef]
4. Zolfaghari, B.; Singh, V.; Rai, B.K.; Bibak, K.; Koshiba, T. Cryptography in hierarchical coded caching: System model and cost analysis. *Entropy* **2021**, *23*, 1459. [CrossRef]
5. Liu, Z.; Seo, H. Iot-nums: Evaluating nums elliptic curve cryptography for iot platforms. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 720–729. [CrossRef]
6. He, D.; Zeadally, S.; Kumar, N.; Wu, W. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2052–2064. [CrossRef]
7. Zolfaghari, B.; Bibak, K.; Koshiba, T. The odyssey of entropy: Cryptography. *Entropy* **2022**, *24*, 266. [CrossRef]
8. Bibak, K.; Ritchie, R.; Zolfaghari, B. Everlasting security of quantum key distribution with 1k-dwcdm and quadratic hash. *Quantum Inf. Comput.* **2021**, *21*, 181–202. [CrossRef]
9. Dong, T.; Huang, T. Neural cryptography based on complex-valued neural network. *IEEE Trans. Neural Netw. Learn. Syst.* **2020**, *31*, 4999–5004. [CrossRef]
10. Zolfaghari, B.; Bibak, K.; Nemati, H.R.; Koshiba, T.; Mitra, P. *Statistical Trend Analysis on Physically Unclonable Functions: An Approach via Text Mining*; CRC Press: Boca Raton, FL, USA, 2021.
11. Dai, J.; Hao, X.; Yan, X.; Li, Z. Adaptive false-target recognition for the proximity sensor based on joint-feature extraction and chaotic encryption. *IEEE Sens. J.* **2022**, *11*, 10828–10840. [CrossRef]
12. Sayed, W.S.; Roshdy, M.; Said, L.A.; Radwan, A.G. Design and fpga verification of custom-shaped chaotic attractors using rotation, offset boosting and amplitude control. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *68*, 3466–3470. [CrossRef]
13. Nosov, V.R.; Campaña, J.A.M.; Gómez Mancilla, J.C. Method and algorithm to construct a quasi-chaotic sequence. *IEEE Lat. Am. Trans.* **2019**, *17*, 31–36. [CrossRef]
14. Zhang, L.; Zhu, Y.; Ren, W.; Wang, Y.; Choo, K.K.R.; Xiong, N.N. An energy efficient authentication scheme based on chebyshev chaotic map for smart grid environments. *IEEE Internet Things J.* **2021**, *8*, 17120–17130. [CrossRef]
15. Rao, N.; Xu, X.; Li, S. Hybrid chaotic sequence for qs-cdma system with rake receiver. *J. Syst. Eng. Electron.* **2004**, *15*, 278–282.
16. Dahiya, M.; Kumar, R. A literature survey on various image encryption & steganography techniques. In Proceedings of the First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018.

17. Makki, Q.H.; Abdalla, A.M.; Tamimi, A.A. A survey of image encryption algorithms. In Proceedings of the International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021.
18. Jasra, B.; Moon, A.H. Image encryption techniques: A review. In Proceedings of the 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 29–31 January 2020.
19. Abusukhon, A.; AlZu'bi, S. New direction of cryptography: A review on text-to-image encryption algorithms based on rgb color value. In Proceedings of the Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020.
20. Pavithra, V.; Jeyamala, C. A survey on the techniques of medical image encryption. In Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 13–15 December 2018.
21. Sankpal, P.R.; Vijaya, P.A. Image encryption using chaotic maps: A survey. In Proceedings of the Fifth International Conference on Signal and Image Processing, Bangalore, India, 8–10 January 2014.
22. Deepa, N.R.; Sivamangai, N.M. A state-of-art model of encrypting medical image using dna cryptography and hybrid chaos map—2d zaslavaski map: Review. In Proceedings of the 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 21–22 April 2022.
23. Yadav, K.; Chaware, T. Review of joint encoding and encryption for image transmission using chaotic map, ldpc and aes encryption. In Proceedings of the 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 7–9 October 2021.
24. Suneja, K.; Dua, S.; Dua, M. A review of chaos based image encryption. In Proceedings of the 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019.
25. Bu, Y. Overview of image encryption based on chaotic system. In Proceedings of the 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 28–29 January 2021.
26. Ayad, J.; Hasan, F.S.; Ali, A.H.; Hussein, Z.K.; Abdulkareem, H.J.; Jalil, M.A.; Ahmed, G.; Sadiq, A. Image encryption using chaotic techniques: A survey study. In Proceedings of the International Conference in Advances in Power, Signal, and Information Technology (APSIT), Bhubaneswar, India, 8–10 October 2021.
27. Thein, N.; Nugroho, H.A.; Adji, T.B.; Mustika, I.W. Comparative performance study on ordinary and chaos image encryption schemes. In Proceedings of the International Conference on Advanced Computing and Applications (ACOMP), Ho Chi Minh, Vietnam, 29 November–1 December 2017.
28. Poggi, M.; Tosi, F.; Batsos, K.; Mordohai, P.; Mattoccia, S. On the synergies between machine learning and binocular stereo for depth estimation from images: A survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2021**. [CrossRef]
29. Zhang, X. Deep learning-based multi-focus image fusion: A survey and a comparative study. *IEEE Trans. Pattern Anal. Mach. Intell.* **2021**. [CrossRef]
30. Minaee, S.; Boykov, Y.Y.; Porikli, F.; Plaza, A.J.; Kehtarnavaz, N.; Terzopoulos, D. Image segmentation using deep learning: A survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *44*, 3523–3542. [CrossRef]
31. Su, J.; Kankani, A.; Zajko, G.; Elchouemi, A.; Kurniawan, H. Review of image encryption techniques using neural network for optical security in the healthcare sector-pno system. In Proceedings of the 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia, 25–27 November 2020.
32. Kumar, S.; Singh, B.K.; Akshita; Pundir, S.; Batra, S.; Joshi, R. A survey on symmetric and asymmetric key based image encryption. In Proceedings of the International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 28–29 February 2020.
33. Mudia, H.M.; Chavan, P.V. Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme—Review. In Proceedings of International Conference on Information Security & Privacy, Nagpur, India, 11–12 December 2015.
34. Yang, X.; Li, F.; Liu, H. Ttl-iqa: Transitive transfer learning based no-reference image quality assessment. *IEEE Trans. Multimed.* **2020**, *23*, 4326–4340. [CrossRef]
35. Liu, S.; Liu, S.; Sun, F.S. Spatial chaos-based image encryption design. *Sci. China Ser. Phys. Mech. Astron.* **2009**, *52*, 177–183. [CrossRef]
36. Faragallah, O.S.; Afifi, A.; El-Shafai, W.; El-Sayed, H.S.; Naeem, E.A.; Alzain, M.A.; Al-Amri, J.F.; Soh, B.; El-Samie, F.A. Investigation of chaotic image encryption in spatial and frft domains for cybersecurity applications. *IEEE Access* **2020**, *8*, 42491–42503. [CrossRef]
37. Wang, J.; Chen, G. Design of a chaos-based digitlal image encryption algorithm in time domain. In Proceedings of the IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, India, 13–14 February 2015.
38. Ge, X.; Liu, F.; Lu, B.; Wang, W.; Chen, J. An image encryption algorithm based on spatiotemporal chaos in dct domain. In Proceedings of the 2nd IEEE International Conference on Information Management and Engineering, Chengdu, China, 16–18 April 2010.
39. Luo, Y.; Du, M.; Liu, D. Jpeg image encryption algorithm based on spatiotemporal chaos. In Proceedings of the Fifth International Workshop on Chaos-fractals Theories and Applications, Dalian, China, 18–21 October 2012.
40. He, B.; Zhang, F.; Luo, L.; Du, M.; Wang, Y. An image encryption algorithm based on spatiotemporal chaos. In Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17–19 October 2009.
41. Wang, X.; Feng, L.; Wang, S.; Chuan, Z.; Zhang, Y. Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption. *IEEE Access* **2018**, *6*, 2169–3536.
42. Hou, J.; Xi, R.; Liu, P.; Liu, T. The switching fractional order chaotic system and its application to image encryption. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 381–388. [CrossRef]

43. Wei, J.; Zhang, M.; Tong, X. Image encryption algorithm based on fractional order chaotic system. In Proceedings of the IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 20–22 August 2021.
44. George, R.T.; Gopakumar, K. Spatiotemporal chaos in globally coupled nca map lattices using 3-d arnold cat map for digital image encryption. In Proceedings of the First International Conference on Computational Systems and Communications (ICCSC), Trivandrum, India, 17–18 December 2014.
45. Zhang, Y.; Xie, J.; Sun, P.; Huang, L. A new image encryption algorithm based on arnold and coupled chaos maps. In Proceedings of the International Conference on Computer and Communication Technologies in Agriculture Engineering, Chengdu, China, 12–13 June 2010.
46. Wu, X. A novel chaos-based image encryption scheme using coupled map lattices. In Proceedings of the 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Shenyang, China, 23–25 July 2013.
47. Jiang, H.Y.; Fu, C. An image encryption scheme based on lorenz chaos system. In Proceedings of the Fourth International Conference on Natural Computation, Jinan, China, 18–20 October 2008.
48. Sharma, M.; Bhargava, A. Chaos based image encryption using two step iterated logistic map. In Proceedings of the International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 23–25 December 2016.
49. Lei, L.-H.; Bai, F.-M.; Han, X.-H. New image encryption algorithm based on logistic map and hyper-chaos. In Proceedings of the International Conference on Computational and Information Sciences, Shiyang, China, 21–23 June 2013.
50. Mu, Z.; Liu, H. Research on digital media image encryption algorithm based on logistic chaotic map. In Proceedings of the International Conference on Robots & Intelligent System (ICRIS), Sanya, China, 7–8 November 2020.
51. Wu, X.; Zhu, B.; Hu, Y.; Ran, Y. A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps. *IEEE Access* **2017**, *5*, 6429–6436.
52. Zhu, C.; Sun, K. Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps. *IEEE Access* **2018**, *6*, 18759–18770. [CrossRef]
53. Muhammad, Z.M.Z.; Özkaynak, F. A cryptographic confusion primitive based on lotka–volterra chaotic system and its practical applications in image encryption. In Proceedings of the IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 25–29 February 2020.
54. Tresor, L.O.; Sumbwanyambe, M. A selective image encryption scheme based on 2d dwt, henon map and 4d qi hyper-chaos. *IEEE Access* **2019**, *7*, 103463–103472. [CrossRef]
55. Zeng, H.; Chen, D. Image encryption algorithm based on logistic-sine compound chaos. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Chongqing, China, 29–30 October 2020.
56. Zhao, F.; Li, C.; Liu, C.; Zhang, J. Image encryption algorithm based on sine-logistic cascade chaos. In Proceedings of the 5th International Conference on Control, Automation and Robotics (ICCAR), Beijing, China, 19–22 April 2019.
57. Lu, Q.; Zhu, C.; Deng, X. An efficient image encryption scheme based on the lss chaotic map and single S-box. *IEEE Access* **2020**, *8*, 25664–25678. [CrossRef]
58. Zhu, H.; Zhao, Y.; Song, Y. 2d logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **2019**, *7*, 14081–14098. [CrossRef]
59. Zhang, H.; Zhu, J.; Zhao, S.; He, Q.; Zhong, X.; Liu, J. A new image encryption algorithm based on 2d-lsimm chaotic map. In Proceedings of the 12th International Conference on Advanced Computational Intelligence (ICACI), Dali, China, 14–16 August 2020.
60. Balakrishnan, B.; Mubarak, D.M.N. An improved image encryption using 2d logistic adjusted sine chaotic map with shuffled index matrix. In Proceedings of the International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 19–20 February 2021.
61. Elshamy, A.M.; Rashed, A.N.Z.; Mohamed, A.E.-N.A.; Faragalla, O.S.; Mu, Y.; Alshebeili, S.A.; El-Samie, F.E.A. Optical image encryption based on chaotic baker map and double random phase encoding. *J. Light. Technol.* **2013**, *31*, 2533–2539. [CrossRef]
62. Tong, X.; Liu, Y.; Zhang, M.; Wang, Z. A novel image encryption scheme based on dynamical multiple chaos and baker map. In Proceedings of the 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science, Guilin, China, 19–22 October 2012.
63. Krishna, P.R.; Surya Teja, C.V.M.; Renuga, D.S.; Thanikaiselvan, V. A chaos based image encryption using tinkerbell map functions. In Proceedings of the Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018.
64. Kavinmozhi, G.; Premkumar, R.; Anand, S.; Robinson, S. A hybrid chaos approach for image encryption using ctic map. In Proceedings of the International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, 1–3 March 2018.
65. Savitri, N.; Johan, A.W.S.B.; Islama, F.A.; Utaminingrum, F. Efficient technique image encryption with cipher block chaining and gingerbreadman map. In Proceedings of the International Conference on Sustainable Information Engineering and Technology (SIET), Lombok, Indonesia, 28–30 September 2019.
66. Moysis, L.; Kafetzis, I.; Volos, C.; Tutueva, A.V.; Butusov, D. Application of a hyperbolic tangent chaotic map to random bit generation and image encryption. In Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg and Moscow, Russia, 26–29 January 2021.

67. Bisht, A.; Jaroli, P.; Dua, M.; Dua, S. Symmetric multiple image encryption using multiple new one-dimensional chaotic functions and two-dimensional cat man. In Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018.
68. Wang, X.; Zhu, X.; Zhang, Y. An image encryption algorithm based on josephus traversing and mixed chaotic map. *IEEE Access* **2018**, *6*, 23733–23746. [CrossRef]
69. Fu, C.; Li, W.; Meng, Z.; Wang, T.; Li, P. A symmetric image encryption scheme using chaotic baker map and lorenz system. In Proceedings of the Ninth International Conference on Computational Intelligence and Security, Emeishan, China, 14–15 December 2013.
70. Choi, U.S.; Cho, S.J.; Kang, S.W. Color image encryption algorithm for medical image by mixing chaotic maps. In Proceedings of the 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, 20–22 July 2020.
71. Zhang, X.; Wang, L.; Zhou, Z.; Niu, Y. A chaos-based image encryption technique utilizing hilbert curves and h-fractals. *IEEE Access* **2019**, *7*, 74734–74746. [CrossRef]
72. Aslam, M.N.; Belazi, A.; Kharbech, S.; Talha, M.; Xiang, W. Fourth order mca and chaos-based image encryption scheme. *IEEE Access* **2019**, *7*, 66395–66409.
73. Habibipour, M.; Maarefdoust, R.; Yaghobi, M.; Rahati, S. An image encryption system by 2d memorized cellular automata and chaos mapping. In Proceedings of the 6th International Conference on Digital Content, Multimedia Technology and Its Applications, Seoul, Korea, 16–18 August 2010.
74. Habibipour, M.; Yaghobi, M.; Rahati-Q, S.; souzanchi k, Z. An image encryption system by indefinite cellular automata and chaos. In Proceedings of the 2nd International Conference on Signal Processing Systems, Dalian, China, 5–7 July 2010.
75. García, V.M.S.; Ramírez, M.D.G.; Carapia, R.F.; Vega-Alvarado, E.; Escobar, E.R. A novel method for image encryption based on chaos and transcendental numbers. *IEEE Access* **2019**, *7*, 163729–163739. [CrossRef]
76. Xie, Y.; Li, J.; Kong, Z.; Zhang, Y.; Liao, X.; Liu, Y. Exploiting optics chaos for image encryption-then-transmission. *J. Light. Technol.* **2016**, *34*, 5101–5109. [CrossRef]
77. Liu, X.; Guo, R.; Li, M.; Wei, Z. Research on image encryption in secure communication system of space laser chaos keying. In Proceedings of the International Conference on Wireless Communications and Smart Grid (ICWCSG), Qingdao, China, 12–14 June 2020.
78. Li, L.; Xie, Y.; Liu, Y.; Liu, B.; Ye, Y.; Song, T.; Zhang, Y.; Liu, Y. Exploiting optical chaos for color image encryption and secure resource sharing in cloud. *IEEE Photonics J.* **2019**, *11*, 1–11. [CrossRef]
79. Liu, B.; Xie, Y.; Zhang, Y.; Ye, Y.; Song, T.; Liao, X.; Liu, Y. Arm-embedded implementation of a novel color image encryption and transmission system based on optical chaos. *IEEE Photonics J.* **2020**, *12*, 1–12. [CrossRef]
80. AlMutairi, F.; Bonny, T. Image encryption based on chua chaotic oscillator. In Proceedings of the International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 25–26 November 2020.
81. Lin, Z.H.; Wang, H.X. Image encryption based on chaos with pwl memristor in chua's circuit. In Proceedings of the International Conference on Communications, Circuits and Systems, Milpitas, CA, USA, 23–25 July 2009.
82. Liu, Z.; Wu, C.; Wang, J.; Hu, Y. A color image encryption using dynamic dna and 4-d memristive hyper-chaos. *IEEE Access* **2019**, *7*, 78367–78378. [CrossRef]
83. Sun, J.; Li, C.; Lu, T.; Akgul, A.; Min, F. A memristive chaotic system with hypermultistability and its application in image encryption. *IEEE Access* **2020**, *8*, 139289–139298. [CrossRef]
84. Muhammad, A.S.; Özkaynak, F. Siea: Secure image encryption algorithm based on chaotic systems optimization algorithms and pufs. *Symmetry* **2021**, *13*, 824. [CrossRef]
85. Wang, X.; Liu, P. A new image encryption scheme based on a novel one-dimensional chaotic system. *IEEE Access* **2020**, *8*, 174463–174479. [CrossRef]
86. Elghandour, A.N.; Salah, A.M.; Elmasry, Y.A.; Karawia, A.A. An image encryption algorithm based on bisection method and one-dimensional piecewise chaotic map. *IEEE Access* **2021**, *9*, 43411–43421. [CrossRef]
87. Tiwari, H.; Satish, K.N.; Harshitha, R.; Shilpa, N.; Rakshatha, S.; Archana, K.N. Ensuring confidentiality in bsn with 1-d chaos based image encryption scheme. In Proceedings of the International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018.
88. Yang, S.; Tong, X. A block image encryption algorithm based on 2d chaotic system. In Proceedings of the IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 20–22 August 2021.
89. Qian, X.; Yang, Q.; Li, Q.; Liu, Q.; Wu, Y.; Wang, W. A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. *IEEE Access* **2021**, *9*, 61334–61345. [CrossRef]
90. Asl, A.M.; Broumandnia, A.; Mirabedini, S.J. Scale invariant digital color image encryption using a 3d modular chaotic map. *IEEE Access* **2021**, *9*, 102433–102449.
91. Cao, Y.y.; Fu, C. An image encryption scheme based on high dimension chaos system. In Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA), Changsha, China, 20–22 October 2008.
92. Mu, X.; E-Nuo, S. A new color image encryption algorithm based on 3d lorenz chaos sequences. In Proceedings of the First International Conference on Pervasive Computing, Signal Processing and Applications, Harbin, China, 17–19 September 2010.

93. Huang, Y.; Huang, L.; Wang, Y.; Peng, Y.; Yu, F. Shape synchronization in driver-response of 4-d chaotic system and its application in image encryption. *IEEE Access* **2020**, *8*, 135308–135319. [CrossRef]
94. Zhu, S.; Zhu, C. Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map. *IEEE Access* **2019**, *7*, 147106–147118. [CrossRef]
95. Qiu, W.C.; Yan, S.J. An image encryption algorithm based on the combination of low-dimensional chaos and high-dimensional chaos. In Proceedings of the 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE), Xiamen, China, 18–20 October 2019.
96. Parida, P.; Pradhan, C.; Gao, X.; Roy, D.S.; Barik, R.K. Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. *IEEE Access* **2021**, *9*, 76191–76204. [CrossRef]
97. Xu, J.; Zhao, C.; Mou, J. A 3d image encryption algorithm based on the chaotic system and the image segmentation. *IEEE Access* **2020**, *8*, 145995–146005. [CrossRef]
98. Firdous, A.; Rehman, A.U.; Missen, M.M.S. A gray image encryption technique using the concept of water waves, chaos and hash function. *IEEE Access* **2021**, *9*, 11675–11693. [CrossRef]
99. Ravichandran, D.; Balasubramanian, V.; Fathima, S.; Banu, A.; Anushiadevi; Amirtharajan, R. Chaos and iwt blended image encryption for grey scale image security. In Proceedings of the International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 30–31 March 2019.
100. Hu, X.; Wei, L.; Chen, W.; Chen, Q.; Guo, Y. Color image encryption algorithm based on dynamic chaos and matrix convolution. *IEEE Access* **2020**, *8*, 12452–12466. [CrossRef]
101. Sun, Y.J.; Zhang, H.; Wang, C.P.; Li, Z.Y.; Wang, X.Y. Networked chaotic map model and its applications in color multiple image encryption. *IEEE Photonics J.* **2020**, *12*, 1–18. [CrossRef]
102. Yin, P.; Min, L. A color image encryption algorithm based generalized chaos synchronization for bidirectional discrete systems for audio signal communication. In Proceedings of the International Conference on Intelligent Control and Information Processing, Dalian, China, 13–15 August 2010.
103. Wang, J. Image encryption algorithm based on 2-d wavelet transform and chaos sequences. In Proceedings of the International Conference on Computational Intelligence and Software Engineering, Wuhan, China, 11–13 December 2009.
104. Zhang, Q.; Shen, M.; Li, B.; Fang, R. Chaos-based color image encryption scheme in the wavelet domain. In Proceedings of the 7th International Congress on Image and Signal Processing, Dalian, China, 14–16 October 2014.
105. Wang, Q.; Ding, Q.; Zhang, Z.; Ding, L. Digital image encryption research based on dwt and chaos. In Proceedings of the Fourth International Conference on Natural Computation, Jinan, China, 18–20 October 2008.
106. Zhang, S.; Cai, R.; Jiang, Y.; Guo, S. An image encryption algorithm based on multiple chaos and wavelet transform. In Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17–19 October 2009.
107. Macovei, C.; Răducanu, M.; Datcu, O. Image encryption algorithm using wavelet packets and multiple chaotic maps. In Proceedings of the International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 5–6 November 2020.
108. Li, X.; Zhang, Y. Digital image encryption and decryption algorithm based on wavelet transform and chaos system. In Proceedings of the IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 3–5 October 2016.
109. Karmakar, J.; Mandal, M.K. Chaos-based image encryption using integer wavelet transform. In Proceedings of the 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 27–28 February 2020.
110. Gao, H.; Wang, X. Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position. *IEEE Access* **2021**, *9*, 105627–105640. [CrossRef]
111. Zhang, L.; Wu, J.; Zhou, N. Image encryption with discrete fractional cosine transform and chaos. In Proceedings of the Fifth International Conference on Information Assurance and Security, Xi'an, China, 18–20 August 2009.
112. Jiang, A.; Yu, J.; Cang, X. Image encryption algorithm based on chaos and contourlet transform. In Proceedings of the First International Conference on Pervasive Computing, Signal Processing and Applications, Harbin, China, 17–19 September 2010.
113. Li, X.M.; Dai, L. Reality-preserving image encryption assosiated with the chaos and the lct. In Proceedings of the 3rd International Congress on Image and Signal Processing, Yantai, China, 16–18 October 2010.
114. Ashtiyani, M.; Birgani, P.M.; Hosseini, H.M. Chaos-based medical image encryption using symmetric cryptography. In Proceedings of the 3rd International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, Syria, 7–11 April 2008.
115. Wu, Z.; Zhang, X.; Zhong, X. Generalized chaos synchronization circuit simulation and asymmetric image encryption. *IEEE Access* **2019**, *7*, 37989–38008. [CrossRef]
116. Bora, S.; Sen, P.; Pradhan, C. Novel color image encryption technique using blowfish and cross chaos map. In Proceedings of the International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 2–4 April 2015.
117. Abbas, A.M.; Alharbi, A.A.; Ibrahim, S. A novel parallelizable chaotic image encryption scheme based on elliptic curves. *IEEE Access* **2021**, *9*, 54978–54991. [CrossRef]
118. Yousif, S.F.; Abboud, A.J.; Radhi, H.Y. Robust image encryption with scanning technology, the el-gamal algorithm and chaos theory. *IEEE Access* **2020**, *8*, 155184–155209. [CrossRef]
119. 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]

120. Dsouza, C.A.; Sonawane, K. Securing folder directory using image encryption by chaos and rijndael algorithm. In Proceedings of the International Conference on Communication information and Computing Technology (ICCICT), Mumbai, India, 25–27 June 2021.
121. Nkapkop, J.D.D.; Effa, J.Y.; Toma, A.; Cociota, F.; Borda, M. Chaos-based image encryption using the rsa keys management for an efficient web communication. In Proceedings of the 12th IEEE International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 27–28 October 2016.
122. Zhang, Y.; Liu, W.; Cao, S.; Zhai, Z.; Nie, X.; Dai, W. Digital image encryption algorithm based on chaos and improved des. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, San Antonio, TX, USA, 11–14 October 2009.
123. Gupta, K.; Gupta, R.; Agrawal, R.; Khan, S. An ethical approach of block based image encryption using chaotic map. *Int. J. Secur. Appl.* **2015**, *9*, 105–122. [CrossRef]
124. Rani, M.; Kumar, S. A novel and efficient approach to encrypt images using chaotic logistic map and stream cipher. In Proceedings of the International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015.
125. Ginting, R.U.; Dillak, R.Y. Digital color image encryption using rc4 stream cipher and chaotic logistic map. In Proceedings of the International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 7–8 October 2013.
126. Goumidi, D.E.; Hachouf, F. Hybrid chaos-based image encryption approach using block and stream ciphers. In Proceedings of the 8th International Workshop on Systems, Signal Processing and Their Applications (WoSSPA), Algiers, Algeria, 12–15 May 2013.
127. Chapaneri, S.; Chapaneri, R. Chaos based image encryption using latin rectangle scrambling. In Proceedings of the Annual IEEE India Conference (INDICON), Pune, India, 11–13 December 2014.
128. Qu, J. Image encryption algorithm based on logistic chaotic scrambling system. In Proceedings of the IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 11–13 September 2020.
129. Zhang, P.; Chen, M.; Zhang, J. Image encryption algorithm of hyper-chaotic system based on spiral scrambling. In Proceedings of the IEEE International Symposium on Product Compliance Engineering-Asia (ISPCE-CN), Chongqing, China, 6–8 November 2020.
130. Krishnamoorthi, R.; Murali, P. Chaos based image encryption with orthogonal polynomials model and bit shuffling. In Proceedings of the International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 20–21 February 2014.
131. Bhadke, A.A.; Kannaiyan, S.; Kamble, V. Symmetric chaos-based image encryption technique on image bit-planes using sha-256. In Proceedings of the Twenty Fourth National Conference on Communications (NCC), Hyderabad, India, 25–28 February 2018.
132. Slimane, N.B.; Bouallegue, K.; Machhout, M. A novel image encryption scheme using chaos, hyper-chaos systems and the secure hash algorithm sha-1. In Proceedings of the International Conference on Control, Automation and Diagnosis (ICCAD), Hammamet, Tunisia, 19–21 January 2017.
133. Liu, J. A novel sensitive chaotic image encryption algorithm based on sha-3 and steganography. In Proceedings of the IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), Chongqing City, China, 28–30 November 2020.
134. Abd-El-Hafiz, S.K.; AbdElHaleem, S.H.; Radwan, A.G. Permutation techniques based on discrete chaos and their utilization in image encryption. In Proceedings of the 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 28 June–1 July 2016.
135. Ping, P.; Fan, J.; Mao, Y.; Xu, F.; Gao, J. A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access* **2018**, *6*, 59108–59130. [CrossRef]
136. Liu, L.; Lei, Y.; Wang, D. A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation. *IEEE Access* **2020**, *8*, 27361–27374. [CrossRef]
137. Liu, L.; Zhang, L.; Jiang, D.; Guan, Y.; Zhang, Z. A simultaneous scrambling and diffusion color image encryption algorithm based on hopfield chaotic neural network. *IEEE Access* **2021**, *7*, 185796–185810. [CrossRef]
138. Koduru, S.C.; Chandrasekaran, V. Integrated confusion-diffusion mechanisms for chaos based image encryption. In Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops, Sydney, NSW, Australia, 8–11 July 2008.
139. Rehman, M.U.; Shafique, A.; Khalid, S.; Hussain, I. Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps. *IEEE Access* **2021**, *9*, 52277–52291. [CrossRef]
140. Hassan, J.M.; Kadhim, F.A. New S-box transformation based on chaotic system for image encryption. In Proceedings of the 3rd International Conference on Engineering Technology and Its Applications (IICETA), Najaf, Iraq, 6–7 September 2020.
141. Wang, D.; Zhang, Y. Image encryption algorithm based on S-boxes substitution and chaos random sequence. In Proceedings of the International Conference on Computer Modeling and Simulation, Macau, China, 20–22 February 2009.
142. Khan, J.S.; Rehman, A.U.; Ahmad, J.; Habib, Z. A new chaos-based secure image encryption scheme using multiple substitution boxes. In Proceedings of the Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 18 December 2015.
143. Lidong, L.; Jiang, D.; Wang, X.; Zhang, L.; Rong, X. A dynamic triple-image encryption scheme based on chaos, S-box and image compressing. *IEEE Access* **2020**, *8*, 210382–210399. [CrossRef]
144. Rehman, A.U.; Firdous, A.; Iqbal, S.; Abbas, Z.; Shahid, M.M.A.; Wang, H.; Ullah, F. A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine. *IEEE Access* **2020**, *8*, 172275–172295. [CrossRef]
145. Guo, J.; Riyono, D.; Prasetyo, H. Improved beta chaotic image encryption for multiple secret sharing. *IEEE Access* **2018**, *6*, 46297–46321. [CrossRef]

146. Zhang, H.; Li, L.; Li, Q. Reversible data hiding in encrypted images based on block-wise multi-predictor. *IEEE Access* **2021**, *9*, 61943–61954. [CrossRef]
147. Qu, L.; Chen, F.; Zhang, S.; Hongjie, H. Cryptanalysis of reversible data hiding in encrypted images by block permutation and co-modulation. *IEEE Trans. Multimed.* **2021**, *24*, 2924–2937.
148. Wang, Y.; Cai, Z.; He, W. High capacity reversible data hiding in encrypted image based on intra-block lossless compression. *IEEE Trans. Multimed.* **2021**, *23*, 1466–1473. [CrossRef]
149. Xiong, L.; Han, X.; Yang, C.N.; Shi, Y.Q. Robust reversible watermarking in encrypted image with secure multi-party based on lightweight cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 75–91. [CrossRef]
150. Wang, Y.; Cai, Z.; He, W. A new high capacity separable reversible data hiding in encrypted images based on block selection and block-level encryption. *IEEE Access* **2019**, *7*, 175671–175680. [CrossRef]
151. Huang, Z.; Zhang, M.; Zhang, Y. Toward efficient encrypted image retrieval in cloud environment. *IEEE Access* **2019**, *7*, 174541–174550. [CrossRef]
152. Tong, Q.; Miao, Y.; Chen, L.; Weng, J.; Liu, X.; Choo, K.-K.R.; Deng, R. Vfirm: Verifiable fine-grained encrypted image retrieval in multi-owner multi-user settings. *IEEE Trans. Serv. Comput.* **2021**. [CrossRef]
153. Zhang, X. Lossy compression and iterative reconstruction for encrypted image. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 53–58. [CrossRef]
154. Qin, C.; Zhou, Q.; Cao, F.; Dong, J.; Zhang, X. Flexible lossy compression for selective encrypted image with image inpainting. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *29*, 3341–3355. [CrossRef]
155. Bowley, J.; Rebollo-Neira, L. Sparsity and "something else": An approach to encrypted image folding. *IEEE Signal Process. Lett.* **2011**, *18*, 189–192. [CrossRef]
156. Khan, J.S.; Boulila, W.; Ahmad, J.; Rubaiee, S.; Rehman, A.U.; Alroobaea, R.; Buchanan, W.J. Dna and plaintext dependent chaotic visual selective image encryption. *IEEE Access* **2020**, *8*, 159732–159744. [CrossRef]
157. Niu, Y.; Zhang, X. A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation. *IEEE Access* **2020**, *8*, 22082–22093. [CrossRef]
158. Fu, C.; Hou, S.; Zhou, W.; Liu, W.Q.; Wang, D.l. A chaos-based image encryption scheme with a plaintext related diffusion. In Proceedings of the 9th International Conference on Information, Communications & Signal Processing, Tainan, Taiwan, 10–13 December 2013.
159. 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]
160. Yan-Qing, Y.; Zhuo-Min, L. Chosen plaintext attacking on a hyper-chaos image encryption algorithm. In Proceedings of the IEEE 4th International Conference on Electronics Information and Emergency Communication, Beijing, China, 15–17 November 2013.
161. Feng, W.; He, Y. Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on dna encoding and scrambling. *IEEE Photonics J.* **2018**, *10*, 1–15. [CrossRef]
162. Liu, Y.; Qin, Z.; Wu, J. Cryptanalysis and enhancement of an image encryption scheme based on bit-plane extraction and multiple chaotic maps. *IEEE Access* **2019**, *7*, 74070–74080. [CrossRef]
163. 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]
164. Li, M.; Lu, D.; Wen, W.; Ren, H.; Zhang, Y. Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata. *IEEE Access* **2018**, *6*, 47102–47111. [CrossRef]
165. Muhammad, Z.M.Z.; Özkaynak, F. Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique. *IEEE Access* **2019**, *7*, 99945–99953. [CrossRef]
166. Hraoui, S.; Gmira, F.; Jarar, A.O.; Satori, K.; Saaidi, A. Benchmarking aes and chaos based logistic map for image encryption. In Proceedings of the ACS International Conference on Computer Systems and Applications (AICCSA), Ifrane, Morocco, 27–30 May 2013.
167. Nath, S.; Som, S.; Negi, M. Lca approach for image encryption based on chaos to secure multimedia data in iot. In Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019.
168. Boutros, A.; Hesham, S.; Georgey, B. Hardware acceleration of novel chaos-based image encryption for iot applications. In Proceedings of the 29th International Conference on Microelectronics (ICM), Beirut, Lebanon, 10–13 December 2017.
169. 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]
170. Mostafa, S.; Fahim, M.A.N.I.; Hossain, A.B.M.A. A new chaos based medical image encryption scheme. In Proceedings of the 6th International Conference on Informatics, Electronics and Vision & 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT), Himeji, Japan, 1–3 December 2017.
171. Kumari, K.S.; Nagaraju, C. Dna encrypting rules with chaotic maps for medical image encryption. In Proceedings of the 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021.
172. Naveenkumar, S.K.; Panduranga, H.T.; Kiran. Chaos and hill cipher based image encryption for mammography images. In Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015.

173. 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]
174. 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]
175. Han, B.; Jia, Y.; Huang, G.; Cai, L. A medical image encryption algorithm based on hermite chaotic neural network. In Proceedings of the IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020.
176. 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]
177. Ibrahim, A.K.; Hagras, E.A.A.A.; Mohamed, A.N.F.; El-Kamchochi, H.A. Chaotic isomorphic elliptic curve cryptography for secure satellite image encryption. In Proceedings of the International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 13–15 July 2021.
178. Hao, J.; Li, H.; Yan, H.; Mou, J. A new fractional chaotic system and its application in image encryption with dna mutation. *IEEE Access* **2021**, *9*, 52364–52377. [CrossRef]
179. Liu, Q.; Liu, L. Color image encryption algorithm based on dna coding and double chaos system. *IEEE Access* **2020**, *8*, 83596–83610. [CrossRef]
180. Samiullah, M.; Aslam, W.; Nazir, H.; Lali, M.I.; Shahzad, B.; Mufti, M.R.; Afzal, H. An image encryption scheme based on dna computing and multiple chaotic systems. *IEEE Access* **2020**, *8*, 25650–25663. [CrossRef]
181. Ahgue, A.O.; Nkapkop, J.D.D.; Effa, J.Y.; Franz, S.; Adelis, P.; Borda, M. A dna-based chaos algorithm for an efficient image encryption application. In Proceedings of the International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 8–9 November 2018.
182. Awdun, B.; Li, G. The color image encryption technology based on dna encoding & sine chaos. In Proceedings of the International Conference on Smart City and Systems Engineering (ICSCSE), Hunan, China, 25–26 November 2016.
183. Qiuqiong, C.; Yao, D.; Zhiyong, N. An image encryption algorithm based on combination of chaos and dna encoding. In Proceedings of the International Conference on Computer Vision, Image and Deep Learning (CVIDL), Chongqing, China, 10–12 July 2020.
184. Mokhtar, M.A.; Gobran, S.N.; El-Badawy, E.S.A.M. Colored image encryption algorithm using dna code and chaos theory. In Proceedings of the International Conference on Computer and Communication Engineering, Kuala Lumpur, Malaysia, 23–25 September 2014.
185. Das, S.; Mondal, S.N.; Sanyal, M. A novel approach of image encryption using chaos and dynamic dna sequence. In Proceedings of the Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019.
186. Wang, Q.; Zhang, Q.; Zhou, C. A multilevel image encryption algorithm based on chaos and dna coding. In Proceedings of the Fourth International on Conference on Bio-Inspired Computing, Beijing, China, 16–19 October 2009.
187. Niyat, A.Y.; Hei, R.M.H.; Jahan, M.V. Chaos-based image encryption using a hybrid cellular automata and a dna sequence. In Proceedings of the International Congress on Technology, Communication and Knowledge (ICTCK), Mashhad, Iran, 11–12 November 2015.
188. Fu, X.; Liu, B.; Xie, Y.; Li, W.; Liu, Y. Image encryption-then-transmission using dna encryption algorithm and the double chaos. *IEEE Photonics J.* **2018**, *10*, 1–8. [CrossRef]
189. Zhang, L.; Gao, T.; Yang, R. Dna coding and central dogma based image encryption using vigenere cipher and chaos map. In Proceedings of the International Conference on Intelligent Control and Information Processing, Dalian, China, 18–20 August 2014.
190. Chidambaram, N.; Thenmozhi, K.; Rengarajan, A.; Vineela, K.; Murali, S.; Vandana, V.; Raj, P. Dna coupled chaos for unified color image encryption—A secure sharing approach. In Proceedings of the Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 20–21 April 2018.
191. Guo, L.; Chen, J.; Li, J. Chaos-based color image encryption and compression scheme using dna complementary rule and chinese remainder theorem. In Proceedings of the 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 16–18 December 2016.
192. Gasimov, V.A.; Mammadov, J.I. Image encryption algorithm using dna pseudo-symbols and chaotic map. In Proceedings of the 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021.
193. Iqbal, N.; Naqvi, R.A.; Atif, M.; Khan, M.A.; Hanif, M.; Abbas, S.; Hussain, D. On the image encryption algorithm based on the chaotic system, dna encoding, and castle. *IEEE Access* **2021**, *9*, 118253–118270. [CrossRef]
194. Özkaynak, F.; Özer, A.B.; Yavuz, S. Security analysis of an image encryption algorithm based on chaos and dna encoding. In Proceedings of the 21st Signal Processing and Communications Applications Conference (SIU), Haspolat, Turkey, 24–26 April 2013.
195. Xu, J.; Li, P.; Yang, F.; Yan, H. High intensity image encryption scheme based on quantum logistic chaotic map and complex hyperchaotic system. *IEEE Access* **2019**, *7*, 167904–167918. [CrossRef]
196. Shao, W.; Cheng, M.; Luo, C.; Deng, L.; Zhang, M.; Fu, S.; Tang, M.; Liu, D. An image encryption scheme based on hybrid electro-optic chaotic sources and compressive sensing. *IEEE Access* **2019**, *7*, 156582–156591. [CrossRef]
197. Zhu, S.; Zhu, C.; Wang, W. A novel image compression-encryption scheme based on chaos and compression sensing. *IEEE Access* **2019**, *6*, 67095–67107. [CrossRef]

198. Toktas, A.; Erkan, g.; Toktas, F.; Yetgın, Z. Chaotic map optimization for image encryption using triple objective differential evolution algorithm. *IEEE Access* **2021**, *9*, 127814–127832. [CrossRef]
199. Giesl, J.; Behal, L.; Vlcek, K. Hardware solution of chaos based image encryption. In Proceedings of the 12th International Symposium on Design and Diagnostics of Electronic Circuits & Systems, Liberec, Czech Republic, 15–17 April 2009.
200. Paliwal, A.; Mohindroo, B.; Suneja, K. Hardware design of image encryption and decryption using cordic based chaotic generator. In Proceedings of the 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 1–3 December 2020.
201. Zhang, Y.; Liu, Z.; Zheng, X. A chaos-based image encryption asic using reconfigurable logic. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems, Macao, China, 30 November–3 December 2008.
202. Hassan, H.S.; Ismail, S.M. Floating-point double-humped chaotic image encryption on FPGA. In Proceedings of the Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 24–26 October 2020.
203. Barakat, M.L.; Radwan, A.G.; Salama, K.N. Hardware realization of chaos based block cipher for image encryption. In Proceedings of the International Conference on Microelectronics, Hammamet, Tunisia, 19–22 December 2011.
204. Gu, Z.; Li, H.; Khan, S.; Deng, L.; Du, X.; Guizani, M.; Tian, Z. Iepsbp: A cost-efficient image encryption algorithm based on parallel chaotic system for green iot. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 89–106. [CrossRef]
205. Fu, C.; Zhang, G.Y.; Zhu, M.; Cong, L.Y.; Lei, W.M. A novel parallel image encryption scheme using chaos. In Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications and IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), Guangzhou, China, 12–15 December 2017.
206. Mohamed, A.G.; Korany, N.O.; El-Khamy, S.E. New dna coded fuzzy based (dnafz) S-boxes: Application to robust image encryption using hyper chaotic maps. *IEEE Access* **2021**, *9*, 14284–14305. [CrossRef]
207. Wang, B.; Nie, J.; He, Z. A transiently chaotic neural-network implementation of the cdma multiuser detector. *IEEE Trans. Neural Netw.* **1999**, *10*, 1257–1259. [CrossRef]
208. Wang, B.; He, Z.; Nie, J. To implement the cdma multiuser detector by using transiently chaotic neural network. *IEEE Trans. Aerosp. Electron. Syst.* **1997**, *33*, 1068–1071. [CrossRef]
209. Cao, Y.; Liu, S.; Liu, X. Optimization of sf/sub 6/circuit breaker based on chaotic neural network. *IEEE Trans. Magn.* **2006**, *42*, 1151–1154.
210. Zhang, C.; Yu, Y.; Wang, Y.; Han, Z.; Zhou, M. Chaotic neural network-based hysteresis modeling with dynamic operator for magnetic shape memory alloy actuator. *IEEE Trans. Magn.* **2021**, *57*, 12–25. [CrossRef]
211. Kong, G.; Fan, H. Enhanced facade parsing for street-level images using convolutional neural networks. *IEEE Trans. Geosci. Remote Sens.* **2020**, *59*, 10519–10531. [CrossRef]
212. Zhao, R.; Dong, D.; Wang, Y.; Li, C.; Ma, Y.; Enríquez, V.F. Image-based crowd stability analysis using improved multi-column convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 5480–5489. [CrossRef]
213. Li, H.-C.; Li, S.-S.; Hu, W.-S.; Feng, J.-H.; Sun, W.-W.; Du, Q. Recurrent feedback convolutional neural network for hyperspectral image classification. *IEEE Geosci. Remote Sens. Lett.* **2021**, *19*. [CrossRef]
214. Mei, S.; Chen, X.; Zhang, Y.; Li, J.; Plaza, A. Accelerating convolutional neural network-based hyperspectral image classification by step activation quantization. *IEEE Trans. Geosci. Remote Sens.* **2021**, *60*. [CrossRef]
215. Wang, Y.; Cheng, J.; Zhou, Y.; Zhang, F.; Yin, Q. A multichannel fusion convolutional neural network based on scattering mechanism for polsar image classification. *IEEE Geosci. Remote Sens. Lett.* **2021**, *19*. [CrossRef]
216. Fernandes, F.E.; Yen, G.G. Automatic searching and pruning of deep neural networks for medical imaging diagnostic. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *32*, 5664–5674. [CrossRef]
217. de Souza, I.E.; Falcão, A.X. Learning cnn filters from user-drawn image markers for coconut-tree image classification. *IEEE Geosci. Remote Sens. Lett.* **2021**, *19*. [CrossRef]
218. Song, T.; Zheng, W.; Liu, S.; Zong, Y.; Cui, Z.; Li, Y. Graph-embedded convolutional neural network for image-based eeg emotion recognition. *IEEE Trans. Emerg. Top. Comput.* **2021**. [CrossRef]
219. Lu, Y.; Chen, Y.; Zhao, D.; Liu, B.; Lai, Z.; Chen, J. Cnn-g: Convolutional neural network combined with graph for image segmentation with theoretical analysis. *IEEE Trans. Cogn. Dev. Syst.* **2020**, *13*, 631–644. [CrossRef]
220. Choi, Y.; Sim, J.; Kim, L.S. Cremon: Cryptography embedded on the convolutional neural network accelerator. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 3337–3341. [CrossRef]
221. Duan, X.; Guo, D.; Liu, N.; Li, B.; Gou, M.; Qin, C. A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access* **2020**, *8*, 25777–25788. [CrossRef]
222. Kotapalle, G.R.; Kotni, S. Security using image processing and deep convolutional neural networks. In Proceedings of the IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018.
223. Morris, T.; Chien, T.; Goodman, E. Convolutional neural networks for automatic threat detection in security x-ray images. In Proceedings of the 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018.
224. Seethalakshmi, K.S.; Usha, B.A.; Sangeetha, K.N. Security enhancement in image steganography using neural networks and visual cryptography. In Proceedings of the International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 6–8 October 2021.

225. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. Privacy-preserving deep neural networks using pixel-based image encryption without common security keys. In Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Lanzhou, China, 18–21 November 2019.
226. Ito, H.; Kinoshita, Y.; Kiya, H. Image transformation network for privacy-preserving deep neural networks and its security evaluation. In Proceedings of the IEEE 9th Global Conference on Consumer Electronics (GCCE), Kobe, Japan, 13–16 October 2020.
227. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. On the security of pixel-based image encryption for privacy-preserving deep neural networks. In Proceedings of the IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019.
228. Fezza, S.A.; Keita, M.; Hamidouche, W. Visual quality and security assessment of perceptually encrypted images based on multi-output deep neural network. In Proceedings of the 9th European Workshop on Visual Information Processing (EUVIP), Paris, France, 23–25 June 2021.
229. Yang, F.; Mou, J.; Cao, Y.; Chu, R. An image encryption algorithm based on bp neural network and hyperchaotic system. *China Commun.* **2020**, *17*, 21–28. [CrossRef]
230. Ismail, I.A.; Galal-Edeen, G.H.; Khattab, S.; Bahtity, M.A.E.M.E. Satellite image encryption using neural networks backpropagation. In Proceedings of the 22nd International Conference on Computer Theory and Applications (ICCTA), Alexandria, Egypt, 13–15 October 2012.
231. Wang, W.; Wang, X.; Luo, X.; Yuan, M. Finite-time projective synchronization of memristor-based bam neural networks and applications in image encryption. *IEEE Access* **2018**, *6*, 56457–56476. [CrossRef]
232. Xiao, J.; Wang, W.; Wang, M. Image encryption algorithm based on memristive bam neural networks. In Proceedings of the IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018.
233. Zhou, S. Image encryption technology research based on neural network. In Proceedings of the International Conference on Intelligent Transportation, Big Data and Smart City, Halong Bay, Vietnam, 19–20 December 2015.
234. Lin, J.; Luo, Y.; Liu, J.; Bi, J.; Qiu, S.; Cen, M.; Liao, Z. An image compression-encryption algorithm based on cellular neural network and compressive sensing. In Proceedings of the IEEE 3rd International Conference on Image, Vision and Computing (ICIVC), Chongqing, China, 27–29 June 2018.
235. Liu, X.; Jin, X.; Zhao, Y. Optical image encryption using fractional-order quantum cellular neural networks in a fractional fourier domain. In Proceedings of the 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Huangshan, China, 28–30 July 2018.
236. Lin, M.; Long, F.; Guo, L. Grayscale image encryption based on latin square and cellular neural network. In Proceedings of the Chinese Control and Decision Conference (CCDC), Yinchuan, China, 28–30 May 2016.
237. Hu, G.; Kou, W.; Dong, J.; Peng, J. A novel image encryption algorithm based on cellular neural networks hyper chaotic system. In Proceedings of the IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018.
238. Liu, Y.; Zhang, J.; Tang, W. Noise removal using cohen-grossberg neural network for improving the quality of the decrypted image in color encryption. In Proceedings of the IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011.
239. Kumar, S.; Aid, R. Image encryption using wavelet based chaotic neural network. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21–24 September 2016.
240. Joshi, S.D.; Udupi, V.R.; Joshi, D.R. A novel neural network approach for digital image data encryption/decryption. In Proceedings of the International Conference on Power, Signals, Controls and Computation, Thrissur, India, 3–6 January 2012.
241. Bharadwaj, G.V.S.E.; Vijaya, K.; Balaga, S.K.; Thanikaiselvan, A.V. Image encryption based on neural network architecture and chaotic systems. In Proceedings of the Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018.
242. Ni, R.; Wang, F.; Wang, J.; Hu, Y. Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain. *IEEE Photonics J.* **2021**, *13*, 1–10. [CrossRef]
243. Preethi, P.; Asokan, R. Neural network oriented roni prediction for embedding process with hex code encryption in dicom images. In Proceedings of the 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 18–19 December 2020.
244. Sirichotedumrong, W.; Maekawa, T.; Kinoshita, Y.; Kiya, H. Privacy-preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain. In Proceedings of the IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, 22–25 September 2019.
245. Tan, X.; Xiang, C.; Cao, J.; Xu, W.; Wen, G.; Rutkowski, L. Synchronization of neural networks via periodic self-triggered impulsive control and its application in image encryption. *IEEE Trans. Cybern.* **2021**. [CrossRef]
246. Wen, S.; Zeng, Z.; Huang, T.; Meng, Q.; Yao, W. Lag synchronization of switched neural networks via neural activation function and applications in image encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2015**, *26*, 1493–1502. [CrossRef]
247. Zhang, X.; Sheng, S.; Lu, G.; Zheng, Y. Synchronization for arrays of coupled jumping delayed neural networks and its application to image encryption. In Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, VIC, Australia, 12–15 December 2017.
248. Chen, W.; Luo, S.; Zheng, W.X. Impulsive synchronization of reaction–diffusion neural networks with mixed delays and its application to image encryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 2696–2710. [CrossRef]

249. Wang, W.; Yu, X.; Luo, X.; Kurths, J. Finite-time synchronization of chaotic memristive multidirectional associative memory neural networks and applications in image encryption. *IEEE Access* **2018**, *6*, 35764–35779. [CrossRef]
250. Thoms, G.R.W.; Muresan, R.; Al-Dweik, A. Chaotic encryption algorithm with key controlled neural networks for intelligent transportation systems. *IEEE Access* **2019**, *7*, 158697–158709. [CrossRef]
251. Fang, P.; Liu, H.; Wu, C. A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks. *IEEE Access* **2021**, *9*, 18497–18517. [CrossRef]
252. Huang, Q.; Li, G. Research on the application of image encryption technology based on 7 dimensional cnn hyper chaos. In Proceedings of the International Conference on Smart City and Systems Engineering (ICSCSE), Hunan, China, 25–26 November 2016.
253. Zhang, Y.; Li, B. The memorable image encryption algorithm based on neuron-like scheme. *IEEE Access* **2020**, *8*, 114807–114821. [CrossRef]
254. Xiuhong, W.; Qingli, Q.; Zheng'ou, W. Chaotic neural network technique for "0–1" programming problems. *J. Syst. Eng. Electron.* **2003**, *4*, 99–105.
255. Shiyu, H.; Jianying, X. Shortest path routing algorithm based on chaotic neural network. *J. Syst. Eng. Electron.* **2003**, *14*, 1–6.
256. Zhao, L.; Sun, M.; Cheng, J.; Xu, Y. A novel chaotic neural network with the ability to characterize local features and its application. *IEEE Trans. Neural Netw.* **2009**, *20*, 735–742. [CrossRef]
257. He, Z.; Zhang, Y.; Wei, C.; Wang, J. A multistage self-organizing algorithm combined transiently chaotic neural network for cellular channel assignment. *IEEE Trans. Veh. Technol.* **2002**, *51*, 1386–1396.
258. Zhao, C.; Gan, L. Dynamic channel assignment for large-scale cellular networks using noisy chaotic neural network. *IEEE Trans. Neural Netw.* **2011**, *22*, 222–232. [CrossRef]
259. Sun, M.; Xu, Y.; Dai, X.; Guo, Y. Noise-tuning-based hysteretic noisy chaotic neural network for broadcast scheduling problem in wireless multihop networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2012**, *23*, 1905–1918.
260. Sun, M.; Zhao, L.; Cao, W.; Xu, Y.; Dai, X.; Wang, X. Novel hysteretic noisy chaotic neural network for broadcast scheduling problems in packet radio networks. *IEEE Trans. Neural Netw.* **2010**, *21*, 1422–1433.
261. Wang, L.; Li, S.; Tian, F.; Fu, X. A noisy chaotic neural network for solving combinatorial optimization problems: Stochastic chaotic simulated annealing. *IEEE Trans. Syst. Man Cybern. Part B* **2004**, *34*, 2119–2125. [CrossRef]
262. Wok, T.K.; Smith, K.A. A unified framework for chaotic neural-network approaches to combinatorial optimization. *IEEE Trans. Neural Netw.* **1999**, *10*, 978–981.
263. Kumar, U.; Shukla, S.; Malik, I.; Singh, S.; Bhardwaj, H.; Sakalle, A.; Bhardwaj, A. Image encryption using chaotic neural network. In Proceedings of the 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 17–18 December 2021.
264. 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]
265. He, Y.; Zhang, Y.Q.; He, X.; Wang, X.Y. A new image encryption algorithm based on the of-lstms and chaotic sequences. *Sci. Rep.* **2021**, *11*, 6398. [CrossRef]
266. Zhang, H.; Yang, S. Image encryption based on hopfield neural network and bidirectional flipping. *Comput. Intell. Neurosci.* **2022**, *2022*, 7941448. [CrossRef]
267. Zhang, R.; Yu, L.; Jiang, D.; Ding, W.; Song, J.; He, K.; Ding, Q. A novel plaintext-related color image encryption scheme based on cellular neural network and chen's chaotic system. *Symmetry* **2021**, *2021*, 393. [CrossRef]
268. Li, Y.; Aghvami, A.H.; Dong, D. Intelligent trajectory planning in uav-mounted wireless networks: A quantum-inspired reinforcement learning perspective. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1994–1998. [CrossRef]
269. Dong, D.; Chen, C.; Chu, J.; Tarn, T.J. Robust quantum-inspired reinforcement learning for robot navigation. *IEEE/ASME Trans. Mechatron.* **2012**, *17*, 86–97. [CrossRef]
270. Wei, Q.; Ma, H.; Chen, C.; Dong, D. Deep reinforcement learning with quantum-inspired experience replay. *IEEE Trans. Cybern.* **2021**. [CrossRef]
271. Masuyama, N.; Loo, C.K.; Seera, M.; Kubota, N. Quantum-inspired multidirectional associative memory with a self-convergent iterative learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2018**, *29*, 1058–1068. [CrossRef]
272. Patel, O.P.; Bharill, N.; Tiwari, A.; Prasad, M. A novel quantum-inspired fuzzy based neural network for data classification. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1031–1044. [CrossRef]
273. Yuan, Y.; Ning, H.; Lu, X. Bio-inspired representation learning for visual attention prediction. *IEEE Trans. Cybern.* **2021**, *51*, 3562–3575. [CrossRef]
274. Xu, M.; Chen, F.; Li, L.; Shen, C.; Lv, P.; Zhou, B.; Ji, R. Bio-inspired deep attribute learning towards facial aesthetic prediction. *IEEE Trans. Affect. Comput.* **2021**, *12*, 227–238. [CrossRef]
275. Lehnert, H.; Araya, M.; Carrasco-Davis, R.; Escobar, M.J. Bio-inspired deep reinforcement learning for autonomous navigation of artificial agents. *IEEE Lat. Am. Trans.* **2019**, *17*, 2037–2044. [CrossRef]
276. Tu, Z.; Fei, F.; Deng, X. Bio-inspired rapid escape and tight body flip on an at-scale flapping wing hummingbird robot via reinforcement learning. *IEEE Trans. Robot.* **2021**, *37*, 1742–1751. [CrossRef]
277. Yang, Z.; Jin, Y.; Hao, K. A bio-inspired self-learning coevolutionary dynamic multiobjective optimization algorithm for internet of things services. *IEEE Trans. Evol. Comput.* **2019**, *23*, 675–688. [CrossRef]

278. Gibson, S.; Issac, B.; Zhang, L.; Jacob, S.M. Detecting spam email with machine learning optimized with bio-inspired metaheuristic algorithms. *IEEE Access* **2020**, *8*, 187914–187932. [CrossRef]
279. Duan, H.; Li, P.; Shi, Y.; Zhang, X.; Sun, C. Interactive learning environment for bio-inspired optimization algorithms for uav path planning. *IEEE Trans. Educ.* **2015**, *58*, 276–281. [CrossRef]