Nonlinear Dyn (2024) 112:14719–14744
https://doi.org/10.1007/s11071-024-09816-0

REVIEW

Cryptanalysis of substitution-permutation network based image encryption schemes: a systematic review

Sakshi Dhall · Khushboo Yadav

Received: 16 March 2024 / Accepted: 28 May 2024 / Published online: 20 June 2024

Abstract Modern-day's digital world witnesses large-scale transmissions of various media forms (including images) in resource-constrained environments. The sensitive nature of transmitted images has highlighted the importance of image security. Substitution-Permutation Network (SPN) is a popular encryption design catering to the special needs of images. Several reviews on image encryption schemes exist in literature, but reviews focusing on cryptanalysis of image encryption schemes are rare. This motivated us to conduct this systematic review (period: 2019–2023), exploring the trends of cryptanalysis of SPN-based image encryption schemes. This review presents the state-of-the-art in the domain of design and analysis of image encryption. We also identify and highlight the weak designs in existing schemes and provide suggestions for overcoming these weaknesses to prevent potential cryptanalytic attacks. Ultimately, our goal is to contribute to the ongoing efforts to improve security and resilience of image encryption schemes, offering a significant resource for researchers working in this area.

S. Dhall (✉) · K. Yadav
Department of Mathematics, Jamia Millia Islamia, Delhi 110025, India
e-mail: sakshidhall@gmail.com

K. Yadav
e-mail: khushbooyadavjmi@gmail.com

Keywords Cryptanalysis · Chaos · Chaotic maps · Image encryption schemes · Image security · Substitution-permutation network

1 Introduction

Digital communication has become an integral part of our lives due to increased scale of digitization in almost every sphere of our lives, including banking, defense, education, healthcare, entertainment, e-commerce, space-exploration, and the list is endless. Hence, in the era of massive digital communication, the security of the information shared during communication is paramount. One of the important aspects of security is confidentiality, and encryption [1,2] is a very significant countermeasure to achieve confidentiality.

Also, modern-day communication involves transmission of various media forms like audio, video, images, etc., besides textual data. Visual content like images forms a major proportion of transmissions happening today, including medical diagnostic images for patients, digital forensic images for investigations, satellite imagery for space exploration etc. Given the sensitive nature of such image information, it is essential to encrypt it for providing confidentiality during transmission. Lightweight cryptographic schemes are very useful for image security because of the bulky nature of such data and the fact that these days sensitive images are being frequently communicated using resource-constrained IoT (Internet of Things) devices,

Table 1 Use of chaos in cryptography

Property	Description	Use in cryptography
Sensitive to initial condition(s) and system parameter(s)	Small change in initial condition(s) and/or parameter(s) show unpredictable difference in the generated chaotic stream	Useful for achieving avalanche effect in cryptosystems and hash functions[6]
Similarity to random-like behaviour	Generate random-like sequences	Generation of pseudo-random numbers or for key-stream generation
Deterministic	With same initial condition and system parameters chaotic system generates same sequence	Useful for decryption process
Ergodicity	A point of a moving system will eventually cover all regions in uniform and random manner, within the space in which system operates	Useful for achieving confusion/diffusion property
Topological mixing	The change in the system with respect to time is such that any provided region (open set) of phase space of the system after a period of time overlaps with other given region of the system	

Table 2 Measures to evaluate chaotic behaviour

Measure	Chaotic behaviour
Lyapunov exponent (λ) [7]	$\lambda > 0$
Bifurcation diagram [8]	Should exhibit cascade period-doubling
Kolmogorov-Sinai entropy (H) [9]	$H > 0$

which are low in memory capacity, have a small chip size, and operate under power constraints.

To balance the security and efficiency trade-offs in such image encryption schemes, Substitution-Permutation Network (SPN) [3] employing lightweight operations like XOR (Exclusive OR), shift, modular-arithmetic, etc. is one of the most frequently used designs. Also, these SPN-based image encryption schemes, many a time, are referred to as permutation-diffusion ciphers because of the use of permutation operation(s) followed by a substitution layer achieving diffusion. Further, chaos is commonly used in these permutation-diffusion ciphers for image security. Chaos [4] has inherent properties suitable for application in cryptosystems (outlined in Table 1). There are different measures to determine whether a non-linear dynamical system is chaotic or not, which are summarized in Table 2. Figure 1a shows the change in Lyapunov exponent [5] with change in initial parameter value for logistic map with initial condition $x_0 = 0.112345$ and Fig. 1b shows the corresponding bifurcation diagram. Clearly, Lyapunov exponent is shown to attain positive value (represented by dotted line in Fig. 1) for $r \in [3.57, 4)$.

As a result of the above-described properties of chaos, cryptography is witnessing a significantly increased use of chaos in recent past, and its potential is noteworthy in post-quantum cryptography as well [10]. Further, the application of chaotic maps is specifically very popular in image encryption schemes. Initially, 1-D chaotic maps were frequently used, but over a period of time, multidimensional chaotic maps have gained popularity. Details of some of the popular chaotic maps are summarised in the Table 3.

Due to chaos-generated sequences being random-like, they are frequently used as key-streams for substitution/permutation steps during the encryption process (Fig. 2).

In the ever-evolving landscape of information security, besides proposing new encryption schemes, researchers are also equally focusing on the cryptanalysis of existing schemes with an intention to enhance security. Cryptanalysis involves analyzing cryptographic systems to uncover potential vulnerabilities or weaknesses in their design to breach security. The primary objectives of cryptanalysis are:

- **Exploiting weaknesses:** Identifying flaws in cryptographic algorithms or protocols that can be leveraged to bypass their security measures.
- **Key recovery:** Attempting to deduce cryptographic keys fully/partly from available information.

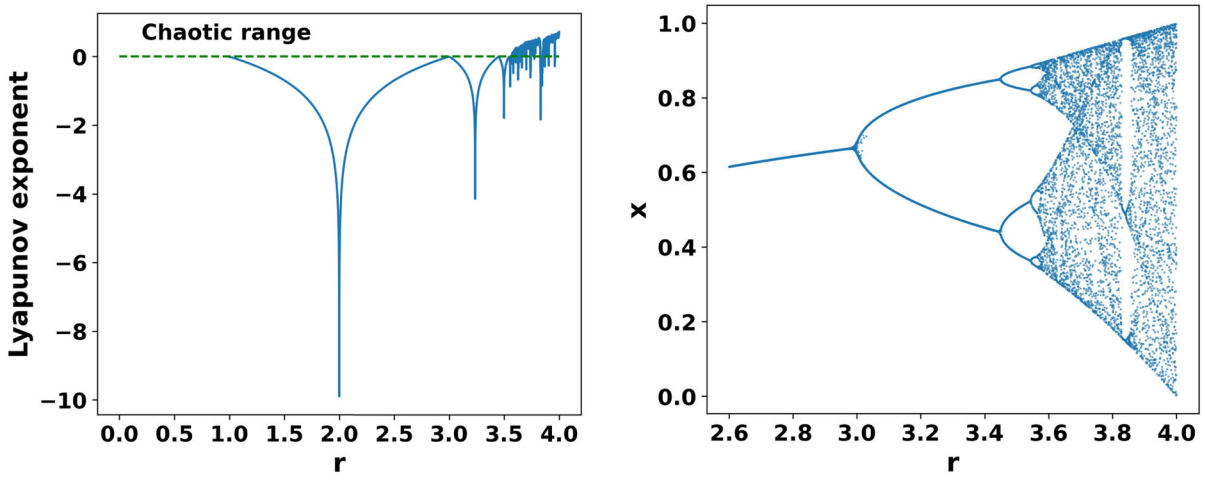


Fig. 1 **a** Lyapunov exponent. **b** Bifurcation diagram of Logistic map with $x_0 = 0.112345$

Table 3 Some popular chaotic maps

Chaotic map	Mathematical expression	Dimension	Chaotic range for initial parameter(s)/condition(s)
Logistic map [11]	$x_{n+1} = r x_n(1 - x_n)$	1	$r \in [3.57, 4)$
Tent map [12]	$x_{n+1} = \begin{cases} \mu x_n & \text{for } 0 \le x_n < \frac{1}{2} \\ \mu(1 - x_n) & \text{for } \frac{1}{2} \le x_n < 1 \end{cases}$	1	$\mu \in [0.6, 2)$
Arnold's cat map [13]	$x_{n+1}, y_{n+1} = 2x_n + y_n, x_n + y_n$	2	No parameter
Baker's map [14]	$x_{n+1}, y_{n+1} = \begin{cases} (2x_n, \frac{y_n}{2}) & \text{for } 0 \le x_n < \frac{1}{2} \\ (2 - 2x_n, 1 - \frac{y_n}{2}) & \text{for } \frac{1}{2} \le x_n < 1 \end{cases}$	2	No parameter
Gingerbreadman map [15]	$x_{n+1} = 1 - y_n + \lvert x_n \rvert \quad y_{n+1} = x_n$	2	No parameter
Lorenz system [16]	$x_{n+1} = \sigma(y_n - x_n) y_{n+1} = x_n(\rho - z_n) - y_n z_{n+1} = x_n y_n - \beta z_n$	3	$\sigma = 10, \beta = \frac{8}{3}, \rho > 24.79$
Rossler system [17]	$x_{n+1} = -y_n - z_n \quad y_{n+1} = x_n + a y_n \quad z_{n+1} = b + z_n(x_n - c)$	3	$a \in [0.33, 0.557], b = 2, c = 4$

- **Breaking encryption:** Attempting to decrypt the targeted ciphertext without knowledge of the corresponding decryption key to recover fully/partly the plaintext.

Cryptanalysis plays a vital role in evaluating the security of cryptographic systems, identifying potential weaknesses, and driving improvements in their design. As technology evolves, new attack techniques, computational advancements, or mathematical breakthroughs may make existing schemes more vulnerable [18]. Researchers continuously work to analyze and discover potential weaknesses in existing cryptographic algorithms [19–21], which leads to the improvement of existing designs or the development of new more secure schemes [22]. Table 4 summarizes few of the basic cryptanalytic attacks.

It is identified that existing literature lacks systematic reviews focusing on the cryptanalysis of image encryption methods. To the best of our knowledge, there is only one review article in existing literature that provides a review on cryptanalysis of image encryption schemes, that too of schemes published only dur-

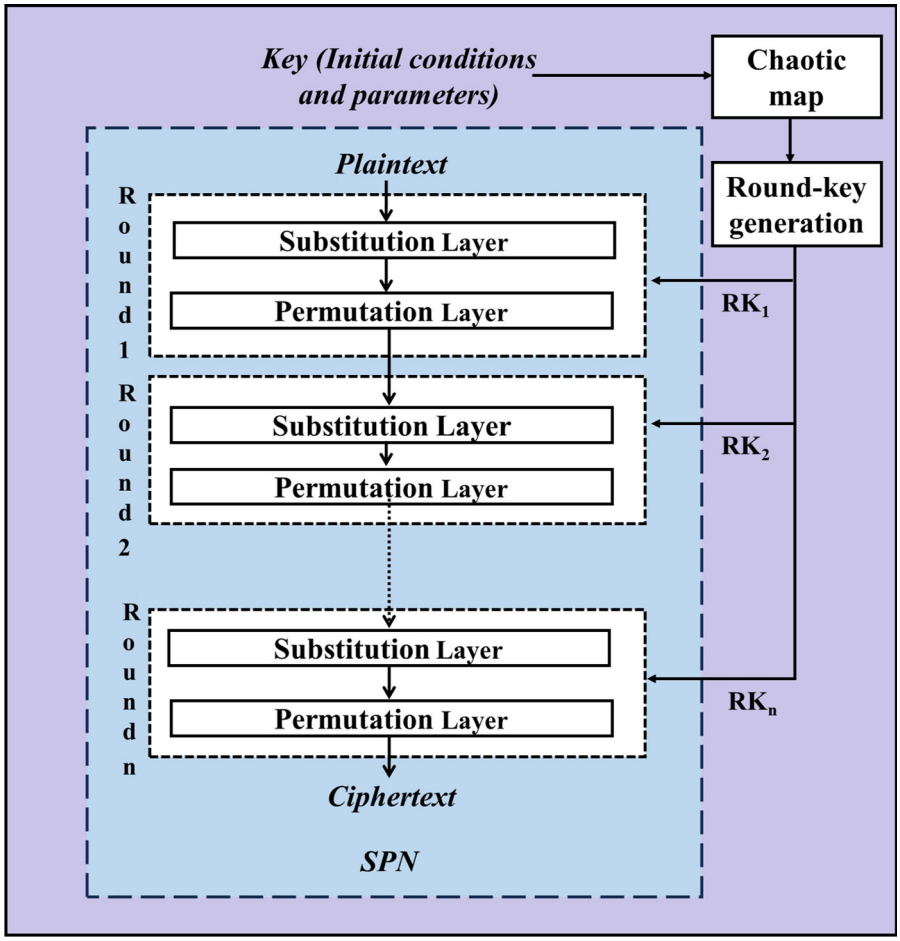


Fig. 2 SPN structure employing chaos for encryption

Table 4 Cryptanalytic attacks

Attack	Description
Ciphertext-only attack [1]	Cryptanalyst has access to only ciphertext and he/she tries to recover the key and/or the plaintext (fully/partly)
Known-plaintext attack [1]	Cryptanalyst has access to known plaintext-ciphertext pair(s)
Chosen-plaintext attack [1]	Cryptanalyst has ability to choose plaintext(s) and find their corresponding ciphertext(s)
Related-key attack [1]	Cryptanalyst knows some relationship between multiple keys, and the cryptanalyst exploits this relationship to recover information about the key and/or the plaintext
Side Channel Attack [1]	Cryptanalyst tries to observe power consumption, temperature, frequency etc., tries to identify some statistical relationship between these parameters and encryption operations to recover the key and/or plaintext
Linear Cryptanalysis [23]	It is a known-plaintext attack in which cryptanalyst utilizes the high probability occurrence of some specific linear expressions (involving bits of the plaintext, ciphertext and secret key) in order to perform cryptanalysis
Differential Cryptanalysis [23]	It is a chosen-plaintext attack where comparison of the differentials in input(s) with differentials in corresponding encrypted output(s) is made in order to recover information about the key and/or the plaintext

Table 5 Comparative analysis of our review with other similar articles in literature

Comparing parameter	[24]	[25]	Our review paper
Is it review article?	Yes	No	Yes
Period	2018	Not specified	2019-23
Primary focus	Cryptanalysis	Key-space analysis	Cryptanalysis
Article selection methodology	The most representative works	Not specified	As per PRISMA guidelines [26]
Plaintext type	Image	Image	Image
Schemes included beyond chaos-based?	Yes	No	Yes
Are improvements suggested?	Yes	Yes	Yes

ing the year 2018 [24]. Also, though not cryptanalysis, a recent paper [25] performed key-space analysis of various image encryption schemes. Table 5 shows the comparative analysis between [24], [25] and our review paper.

Clearly, there was a gap in the literature for comprehensive reviews on cryptanalysis of image encryption schemes over a broader time frame. This motivated us to carry out this systematic review on cryptanalysis of image encryption schemes for the last 5 years, i.e., 2019–23. This review focuses on identifying and highlighting the strengths and weaknesses of image encryption schemes. It also suggests improved designs, and provides an excellent and comprehensive resource for researchers working in the area of image encryption development and cryptanalysis. Following are the research objectives of this systematic review:

- RO1 To present the state-of-the-art in the domain of image encryption schemes and their cryptanalysis.
- RO2 To identify and highlight the weak designs of existing image encryption schemes.
- RO3 To provide suggestions/improvements to mitigate the identified weaknesses to avoid potential cryptanalytic attacks.

The relevance of reviews in the area of image security is highlighted by the ongoing research advancements in this area. New encryption schemes [27,28] are actively being proposed by researchers, and new cryptanalytic attacks [29–34] are also emerging in parallel, as is evident from the most recent literature. While these developments are continuous and also extend beyond the time frame covered in this review, they emphasize the ongoing need for robust security measures in image encryption.

Section 2 presents the methodology used. Section 3 gives discussion on the cryptanalysis techniques used in the research articles included as part of this review. Section 4 presents our findings along with the details of our suggestions on improving future designs of image encryption schemes. Further, Sect. 5 discusses the limitations of this review. Lastly, Sect. 6 gives the conclusion.

2 Methodology

To carry out an extensive review of the existing literature, a systematic approach [26] was taken. This systematic review incorporates diverse viewpoints and a wide range of scholarly contributions in the field of cryptanalysis of image encryption schemes. To search for relevant articles, reputable electronic databases, namely Web of Science and Scopus were searched. Firstly, to understand the overall publication trend as per the existing literature, the keywords searched were "cryptanalysis", "cryptanalysis AND encryption scheme", "cryptanalysis AND image encryption scheme", whose query results are shown in Table 6. This publication trend is also depicted graphically in Fig. 3.

Since, the scope of this review is on cryptanalysis of image encryption schemes, hence, we restricted our search for relevant articles (to be included in this review) to the keyword "cryptanalysis AND image encryption scheme". Further, we included articles published during 2019–23 as part of this review. The articles that were found to be duplicates or irrelevant were manually excluded. Figure 4 shows the PRISMA flow diagram for selecting the relevant articles for this review, starting from the ones searched with the key-

Table 6 Keywords and search results

Keywords	No. of articles	
	Web of Science	Scopus
Cryptanalysis	5372	10,061
Cryptanalysis AND Encryption Scheme	1236	1306
Cryptanalysis AND Image Encryption Scheme	681	354

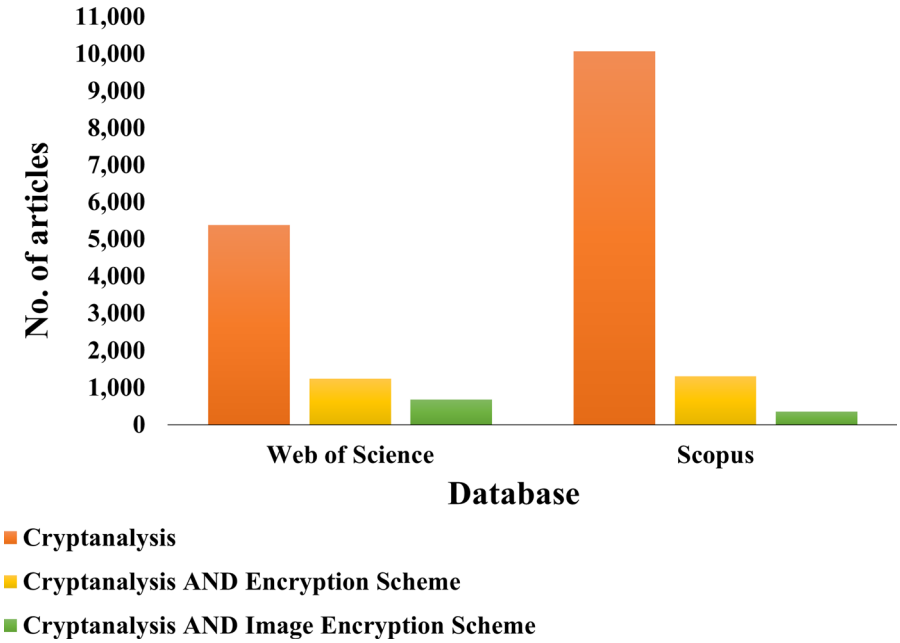


Fig. 3 Publication trend (*as on date 22, December 2023*)

word "cryptanalysis AND image encryption scheme" over the period 2019–23. Figure 5 shows the year-wise count of cryptanalysis articles that are included as the part of this review.

3 Cryptanalysis techniques

During the review, we found that different types of cryptanalytic attacks on the original or reduced equivalent simpler image encryption schemes have been proposed in literature. For better understanding, the classification hierarchy of cryptanalysis articles along with the count of the included articles for each classification is presented in Fig. 6.

Not only the relevant papers on cryptanalysis included in this review were studied, but also the corresponding original image encryption schemes were referred to, during the review. It is observed that the original schemes could be classified on the basis of mathematical primitives, plaintext sensitivity in keys, structure of the schemes based on different combinations of permutation (P) and substitution (S) operations, and number of rounds used in the schemes. Figure 7 shows the classification hierarchy along with the count of referred original image encryption schemes for each classification.

Further, we present the cryptanalysis of these schemes as per the broad three categories, namely, chaos-based, hybrid (using chaos and other mathematical primitives), and others (without chaos). Among the image encryption schemes included in our review, the majority, i.e., 26 schemes, are chaos-based. Additionally, there are 14 schemes that utilise a hybrid approach, i.e. combining chaos with other mathematical primitives. And, only a single scheme is based on non-chaotic mathematical primitives. This observation highlights the prevalent use of chaos in image encryption schemes, with hybrid approaches also being relatively common.

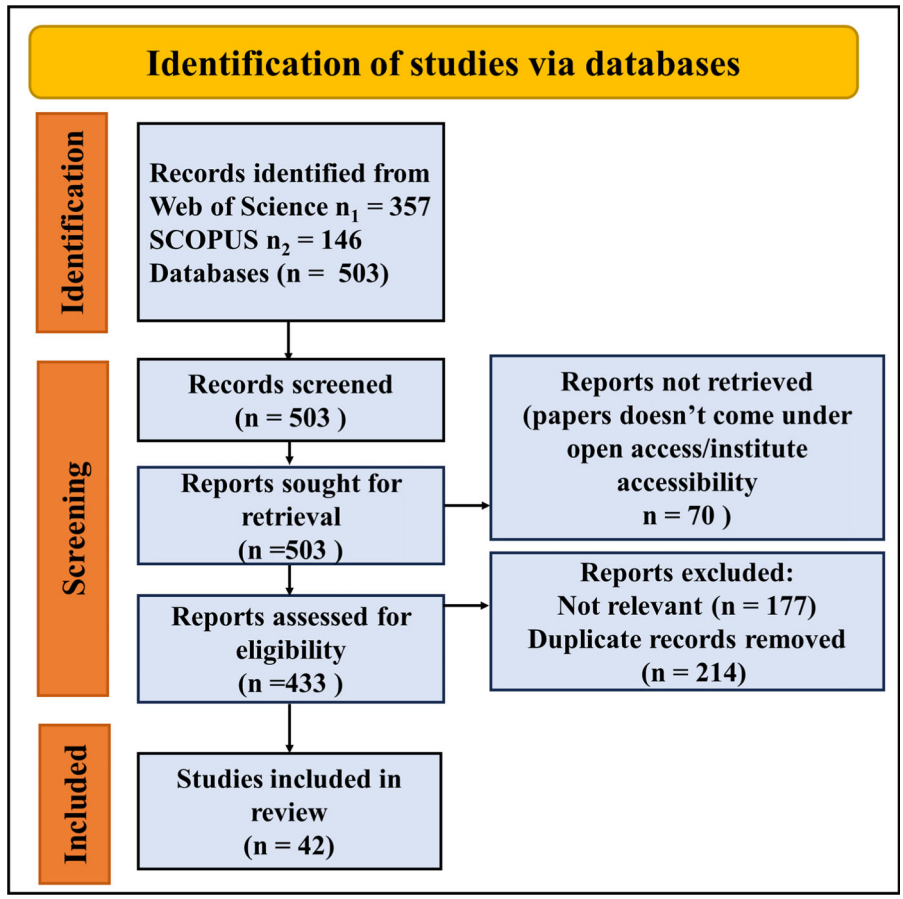


Fig. 4 PRISMA flow diagram

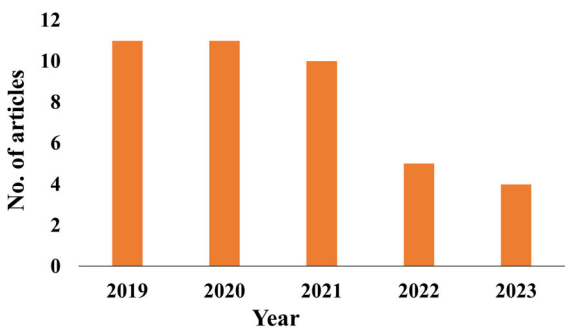


Fig. 5 Year-wise count of included cryptanalysis articles (*as on date 22, December 2023*)

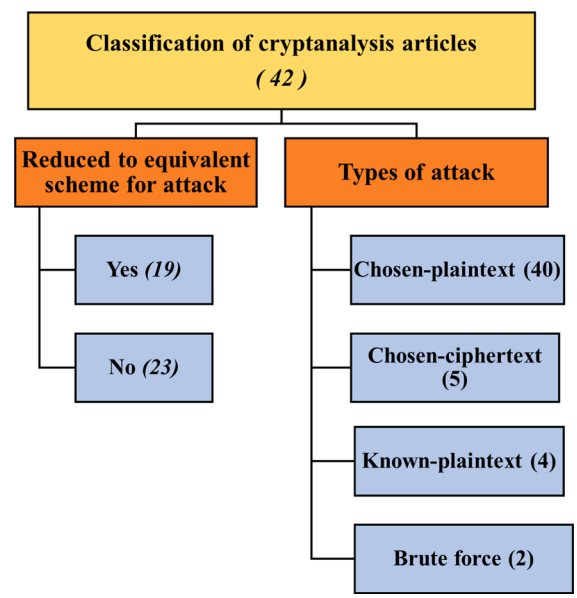


Fig. 6 Classification of included cryptanalysis articles

3.1 Cryptanalysis of chaos-based schemes

In existing image encryption schemes, chaos is majorly utilized for generating key-streams/pseudo-random numbers utilized during encryption process. This subsection focuses on the cryptanalysis of chaos-based image encryption schemes.

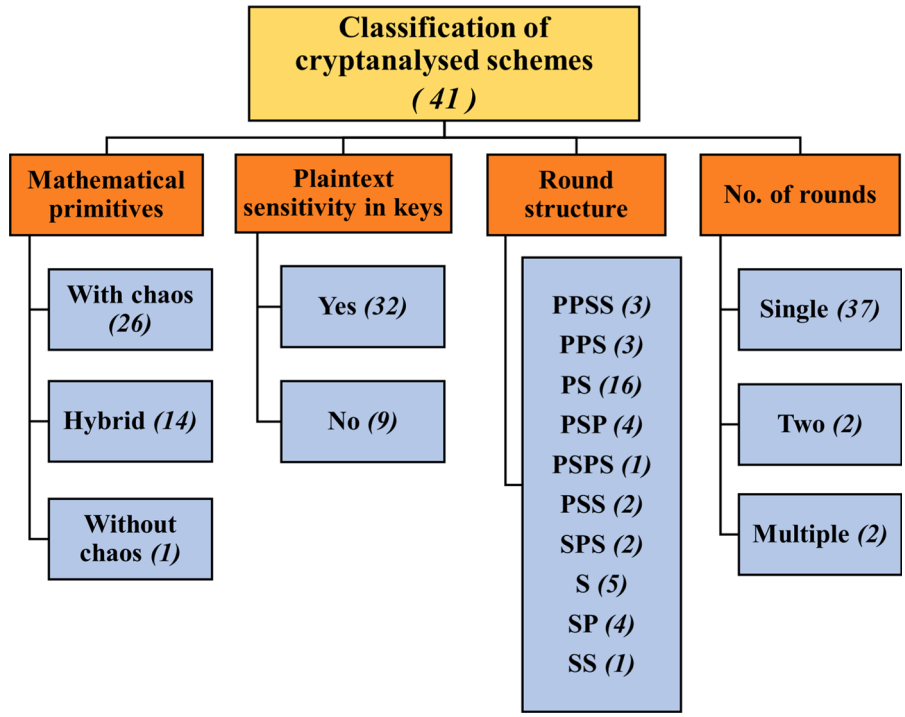


Fig. 7 Classification of cryptanalysed image encryption schemes

Literature reveals that most of the chaos-based schemes are cryptanalysed through chosen-plaintext attack [19–21,35–55] in which the all-zero plain image is one of the most common chosen plain images used to perform the attack [35,41,42,46,47,50,51,53,54,56]. This is because, very commonly, only XOR is used for achieving diffusion after permutation operation(s) in image encryption schemes. And, in an all-zero image, the effect of permutation is nullified, and the obtained ciphertext is the recovered equivalent diffusion key-stream itself as demonstrated using an example in Fig. 8. Like, Zhang et al. [35] cryptanalysed an image encryption scheme [57] which consists of a single round of multiple operations like rotation for permutation and ciphertext feedback-based diffusion through substitution. Also, few researchers have demonstrated chosen-ciphertext attack [35,49,56], differential attack [48] and brute-force attack [46] to cryptanalyse the schemes. Besides a chosen-plaintext attack, Zhang et al. [35] also proposed a chosen-ciphertext attack using plaintext/ciphertext differentials to recover the plain image and the equivalent key-streams.

Further, after recovering the diffusion key-streams and performing the inverse diffusion operation, generally, the permutation mapping between the plain image pixels/bits and the cipher image pixels/bits is recovered with different approaches. It is observed that in most of the cryptanalysed schemes under review, due to weak permutation and diffusion, one plain image pixel contributes to only one cipher image pixel. Hence, not only recovering the diffusion key-stream becomes easy, but recovering the permutation mapping also becomes effortless. For doing this, one of the most common type of attacks on pixel-wise permutation operation is like the one as done by Chen et al. [51]. In this attack (Fig. 9a), multiple chosen plain images having all-zero pixels except one pixel per chosen image are created. All these chosen plain images have the non-zero pixel (say value 1) at different pixel positions, which, after encryption, clearly show their corresponding permuted positions in the obtained respective ciphertexts. Thus, the permutation mapping is easily constructed. An alternate way to recover permutation mapping is proposed by Mukherjee et al. [56]. Here, an $m \times n$ plain image with pixel values ranging from 1 to (mn) is chosen. Comparing the positions of the same pixel values in a plain image and corresponding permuted image provides the permutation key matrix (or mapping). Another approach [50,54] extracts the permutation rule using $q \geq \lceil log_L(m \times n) \rceil$ number of chosen plain images, where L is equal to 2^k for k-bit pixels. In this approach, for example, for a 256 × 256 sized

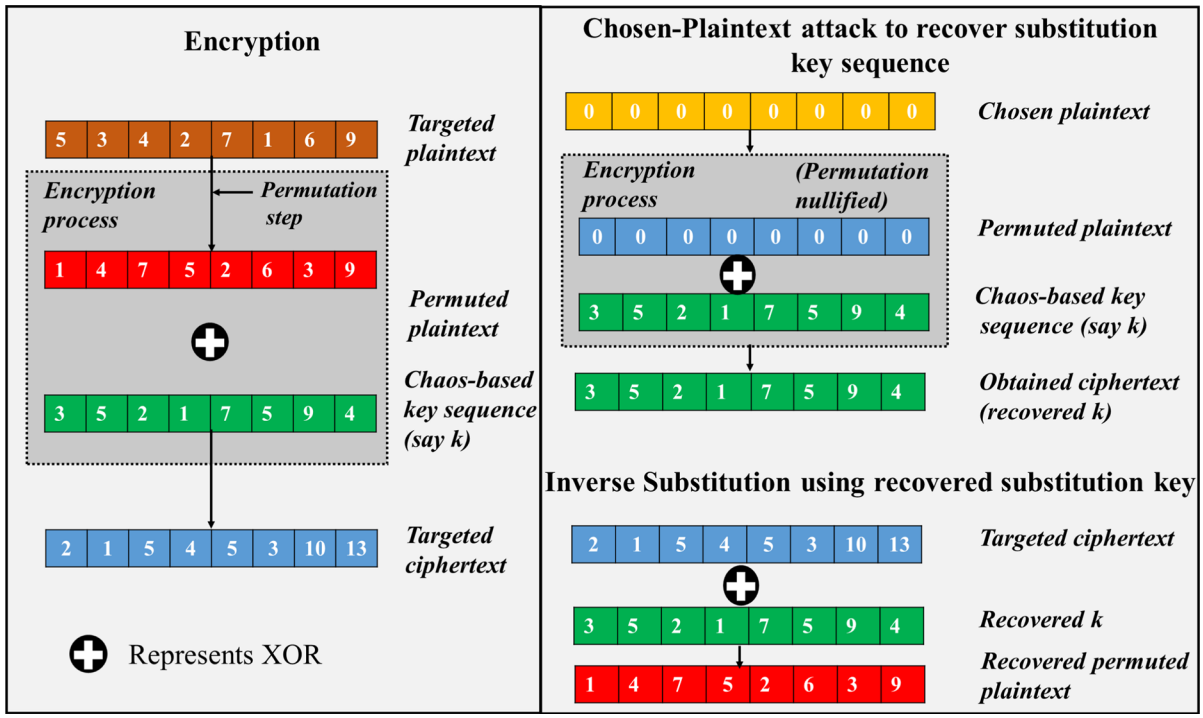
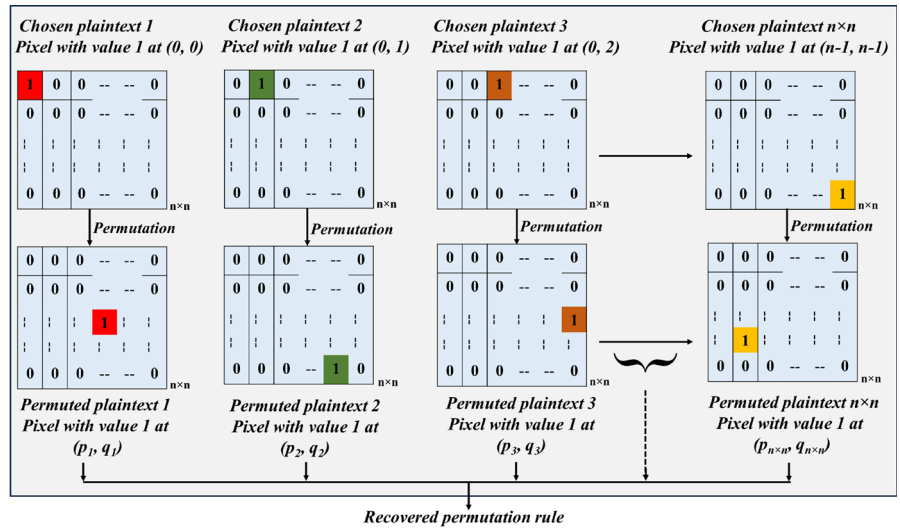


Fig. 8 Example of chosen-plaintext attack to recover substitution key sequence and permuted plaintext (encrypted using a single round SPN)

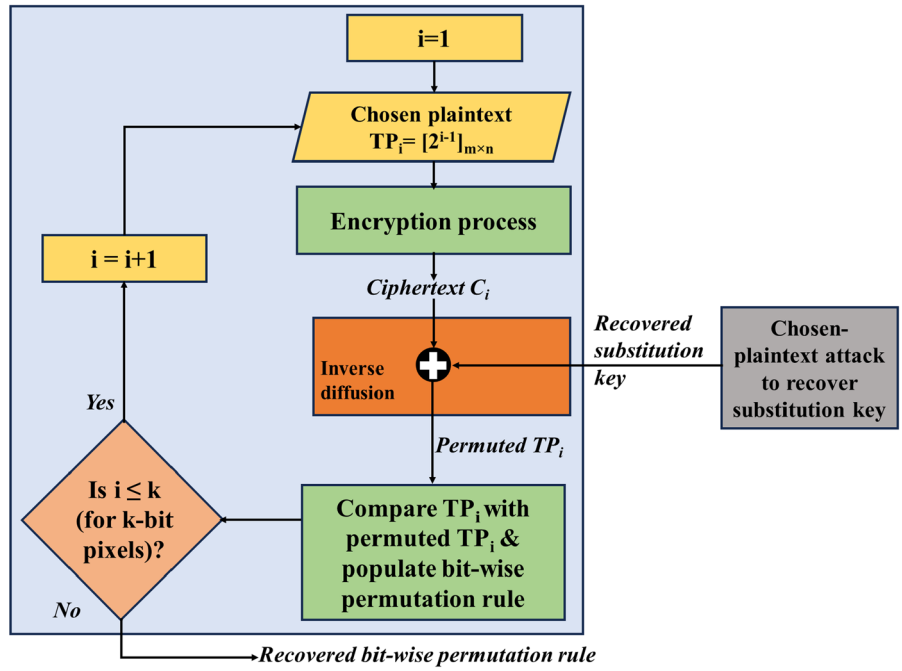
plain image, two chosen plain images, I_1 and $I_2 = I_1^T$ are used. For I_1, the first row's pixel values are 0, the second row's pixel values are 1, and so on until 255. The comparison of I_1 and I_2 with their corresponding permuted plain images provides the required permutation matrix. To recover the bit scrambling sequence for a bit-wise permutation operation, Zhang [53] proposed the use of eight (for $L = 8$) chosen plain images (TP_i) to attack the permutation operation of the scheme [58]. Each chosen plain image TP_i has all pixel values as 2^{i-1}, where i is ranging from 1 to 8. The original scheme [58] employs permutation at pixel level as well as bit level. By virtue of having all same pixel values in each TP_i, the pixel-permutation effect is nullified during encryption, and the bit level comparison of chosen plain images' pixels and their corresponding bit-scrambled images' pixels provides the bit scrambling sequence (Fig. 9b).

As stated earlier, it is highlighted that many of the cryptanalysts have reduced the original encryption schemes into corresponding equivalent encryption schemes for performing cryptanalysis [19,35,36,38,41,46,47,51–55], due to their weak per-round operations. For example, some schemes employ multiple consecutive permutation/substitution operations in each round, which actually provide the strength corresponding to only one equivalent permutation/substitution operation. It is also observed that the schemes employing only a single round [57–77] are frequently targeted for cryptanalysis, while few schemes with two rounds [78,79] or multiple rounds [80,81] have also been cryptanalysed due to their poor confusion/diffusion properties. In fact, our review revealed that there are some of the original schemes [61,80] that had multiple weaknesses and not one, and hence, multiple cryptanalytic attacks were proposed by one or more cryptanalysts [35,36,39,40].

Most cryptanalysed schemes use a single chaotic map to generate key-streams [57,59,62,65,66,68–74,77,79,80], however, some schemes have used multiple chaotic maps as well [58,60,61,63,64,67,75,76]. It is highlighted that irrespective of whether a single chaotic map or multiple chaotic maps is/are used to generate key-streams, the more important aspect is to utilize the generated key-streams effectively during the permutation/substitution operations for providing the desired



(a)



(b)

Fig. 9 **a** Example of chosen-plaintext attack to recover pixel-wise permutation rule. **b** Flowchart for chosen-plaintext attack to recover bit-wise permutation rule

confusion/diffusion properties [55]. However, use of multiple chaotic maps for the key-stream generation can add to the resistance against brute-force attack by way of increasing the key-space size.

3.2 Cryptanalysis of hybrid schemes (other mathematical primitives along with chaos)

For the purpose of enhancing security, some researchers have proposed the use of other mathematical primitives like DNA [82,83], Brownian motion [84], fractals [85] and many more, along with chaos. Despite the use of multiple mathematical primitives, cryptan-

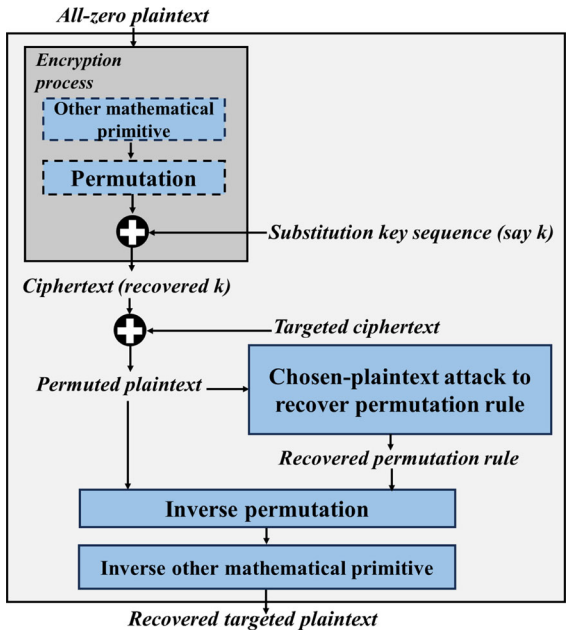


Fig. 10 Block diagram for chosen-plaintext attack on a typical hybrid scheme

alysts have been able to break such schemes due to their poor design. Panwar et al. [86] cryptanalysed the scheme [87] which employs one round of DNA encoding, diffusion, permutation, diffusion, and DNA decoding steps in this order. Kumar and Shankar [88] cryptanalysed the scheme [89] which uses Hill cipher. $C = (AP + X_0)\ mod\ 256$ generates cipher image, where X_0 is a column matrix generated using piecewise linear chaotic map (PWLCM). All-zero plain image nullifies the effect of multiplication with A and provides the key X_0 itself. Then, an identity matrix is chosen as a plain image to extract A. So, Kumar and Shankar demonstrated full recovery of the key which subsequently can be used to decrypt/recover the plaintext.

Figure 10 shows the block diagram for a general attack on a typical hybrid scheme that involves other mathematical primitives along with chaos to recover the plaintext corresponding to the targeted ciphertext.

It is observed that all the cryptanalysed hybrid schemes under review [82–85,87,89–97] used single round of operations, may be for efficiency purposes. However, use of single round makes it easier for cryptanalysts to breach the security [86,88,98–110]. Some schemes use substitution operations only [84,93,95] and are also easily cryptanalysed, like Munir et al. [100] cryptanalysed the scheme [84] which employs only one round of diffusion (substitution) operation. The authors [100] fully recovered the key and the plain image by using known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. As part of the known-plaintext attack, only XOR operation is sufficient to be performed between one known plain image and its corresponding cipher image to recover the entire diffusion key-stream. Further, chosen-plaintext/chosen-ciphertext attack requires a single chosen all-zero plain image/cipher image whose encryption/decryption reveals the entire diffusion key-stream in the form of the obtained cipher image/plain image. While doing cryptanalysis, Munir et al. assumed the effect of the Brownian motion on the generated key-stream to be fixed, whereas the authors of the original scheme Khan et al. [84] specified the effect of the Brownian motion to be time-varying; hence, we find that the cryptanalysis is successful only under the above-mentioned specific assumption. In another work, Zhang et al. [108] cryptanalysed Xu et al.'s scheme [111] which uses logistic map and initial keys to generate Latin cubes. For cryptanalysis a chosen-plaintext attack is performed which recovers the equivalent key-streams by utilising the identified mathematical relationships between the permuted images and the corresponding intermediate ciphertexts.

Also, some of these hybrid schemes utilise plaintext-sensitive keys [82,87,92,94] with an intent to offer higher resistance against cryptanalysis, but they have still been cryptanalysed [20,86,104,106].

Like chaos-based image encryption schemes, most of the hybrid schemes have also been cryptanalysed using chosen-plaintext attacks [86,88,98–109] and, only a few known-plaintext attacks [100,102,107] and chosen-ciphertext attacks [100,109] have been successfully demonstrated in literature.

3.3 Cryptanalysis of scheme without chaos

During our review, we came across only a single image encryption scheme [112] that did not use chaos and only used other mathematical primitives, which has been broken. This scheme uses the Elliptic Curve Cryptography (ECC) for key-matrix generation for the Hill cipher. As the key-space of the original scheme is effectively 2^{32}, hence Lone et al. [22] suggested a brute-force attack to recover the necessary secret keys. Also,

Lone et al. suggested an improvised scheme by firstly replacing Hill cipher by Affine Hill cipher, and then performing permutation and diffusion steps. The key-streams for these permutation and diffusion steps are generated using a 3D variant of Arnold map.

3.4 Summarised observations

The details of the above-mentioned original image encryption schemes and the corresponding cryptanalytic attacks are summarised in tables 7,8,9. Table 7 outlines the design specifications, including the mathematical primitives used, the number of rounds applied, etc., of the cryptanalysed original image encryption schemes. In addition, Table 8 provides the details of the corresponding cryptanalytic attacks. Further, Table 9 specifies the weaknesses of the cryptanalysed image encryption schemes and suggestions as proposed by the corresponding cryptanalysts.

Most of the original scheme articles do not reveal details like the key generation procedure, key sizes, etc., except for a few, due to which their implementation for thorough security analysis becomes difficult. Also, some cryptanalysis papers have hidden assumptions made for the attack [100] which questions the viability of the attack and can also hamper reproducibility for further analysis. Further, many cryptanalysis papers do not perform computational complexity analysis to assess the practicality of the attack in real-world scenarios. It is observed that the original scheme, employing specific round structures like substitution-only (S) and single permutation followed by single substitution (PS), more specifically with simple XOR for substitution, were commonly the ones being cryptanalysed. Additionally, most of the attacked schemes use single-round operations, except a few. Also, most cryptanalysed encryption schemes over-rely on the strength of chaos being used as a mathematical primitive in them. Some schemes also superficially incorporate additional mathematical operations/primitives like Latin cubes, DNA encoding and decoding, matrix multiplication etc. with an aim to enhance security, but to no avail.

4 Results and our contributions

In this section we provide our analysis of the articles made part of this review. Besides presenting the state-of-the-art in the area of image encryption and its cryptanalysis, this review paper has two more major contributions. Firstly, we present our identified weak designs for image encryption schemes which should be avoided in future. Secondly, we propose suggestions for more secure designs. Our findings and suggestions are as under.

4.1 Findings on weak designs in image encryption schemes

We identified weak designs in image encryption schemes prevalent in existing literature which make them vulnerable to cryptanalysis. Following are our findings in this regard:

a Bulkiness and high redundancy are attributed to the image data, so, for efficiency reasons, a majority of the image encryption schemes use chaos to enhance security. But, many a time, there is overreliance on the strength of chaotic systems to add to the security. Due to this overreliance, there is overlooking on part of careful designing of such encryption schemes which leads to their cryptanalysis.

b It is identified that the most common attacks used to cryptanalyse schemes are chosen/known plaintext/ciphertext attacks. These attacks become successful due to the lack of diffusion property, and poor operation designs, which in turn lead to ineffective contribution of key-stream bits in generating the ciphertext. Ultimately, the cipher image pixels do not take contribution from multiple plain image pixels and key-stream bytes.

c To balance the trade-off between security and efficiency, most image encryption schemes opt for a single round of operations. However, relying solely on a single round makes these schemes vulnerable to being reduced to breakable simpler forms susceptible to cryptanalysis. In simpler terms, using just one round of operations might make encryption faster, but it also makes it easier for cryptanalysts to break such a cryptosystem.

d Many cryptanalysts use all black image (all zero image) as chosen plaintext, to perform cryptanalysis. This kind of image nullifies the pixel-wise permutation. Alternatively, they sometimes choose other special plain images to nullify bit-wise permutation (Sect. 3.1). Subsequently, substitution pattern is identified. Such attacks are easy

Table 7 Design specifications of cryptanalysed image encryption schemes

Ref. of scheme	No. of round	Structure	Mathematical primitive/ chaos map used	Operations used during encryption	Plaintext-sensitive key used (yes/no)
[57]	1	PPSS	2D hyperchaotic system	Shifting, modular addition	No
[59]	1	PPS	Kent map	Pixel-wise scrambling, bit-wise scrambling, XOR, modular addition	Yes
[60]	1	PS	Arnold's cat map, Chebyshev map	Pixel-wise scrambling, XOR, modular addition	Yes
[61]	1	PS	Logistic discrete map, Cubic-Logistic map	Bit-wise scrambling, XOR, bit plane composition/decomposition	No
[85]	1	PSS	Julia fractals, 3-D Lorenz map	Pixel-wise scrambling, XOR, multiplication	No
[97]	1	PS	Arnold's map and Lucas series	Pixel-wise scrambling, XOR	No
[87]	1	SPS	Logistic-Tent, Logistic-Sine, Tent-Sine systems and DNA sequences	DNA encoding/decoding, DNA XOR, DNA addition	Yes
[77]	1	PS	Coupled-Sine map	Block-wise scrambling, XOR	No
[90]	1	PS	Logistic map, Arnold's transformation	Pixel-wise scrambling, XOR	No
[81]	Multiple	PS	Logistic map-based Latin square lookup table	Modular addition, lookup operation	No
[78]	2	PS	Random data insertion	Multiple pixel insertions, XOR, modular addition	No
[84]	1	S	Basin map, Gingerbreadman chaotic map and Brownian motion	XOR	No
[62]	1	PSP	Sine-Sine chaotic system	Pixel-wise scrambling, XOR, modular addition, circular shifting	No
[91]	1	PPSS	Henon, Circle, Duffing maps	Intra-block pixel scrambling, block-wise scrambling, XOR	No
[63]	1	PSP	Logistic, Sine, Chebyshev maps	Pixel-wise scrambling, XOR, modular addition, circular rotation	No
[64]	1	PSP	Improved Logistic and improved Sine maps	Bit-plane decomposition/composition, modular addition, XOR, circular rotation	No

Table 7 continued

Ref. of scheme	No. of round	Structure	Mathematical primitive/ chaos map used	Operations used during encryption	Plaintext-sensitive key used (yes/no)
[65]	1	PS	Arnold's cat map	Pixel-wise scrambling, XOR	No
[80]	Multiple	PS	2D Sine-Cosine cross-chaotic map	Pixel-wise scrambling, XOR	No
[66]	1	SP	Third-order hyperbolic Sine system	Pixel-wise scrambling, XOR	No
[67]	1	S	Lorenz, Rossler systems	Lookup table	No
[68]	1	PS	Baker's map	Pixel-wise scrambling, XOR	No
[69]	1	PS	Piece-wise non-linear chaotic map	Pixel-wise scrambling, XOR, modular subtraction	No
[70]	1	PS	Cubic-Logistic map	XOR, modular addition	Yes
[71]	1	PSS	Two-dimensional Sine Logistic modulation map	Pixel-wise scrambling, modular addition	Yes
[72]	1	PS	Logistic map	Bit-wise scrambling, XOR, bit-plane decomposition/composition	No
[92]	1	PS	Lorenz system and hash function	Pixel-wise scrambling, XOR	Yes
[79]	2	S	2D Logistic-adjusted-Sine map	Multiple random pixel insertions, bit-wise scrambling, XOR	No
[83]	1	SPS	4-D hyper-chaotic system	Bit-wise scrambling, DNA XOR, DNA addition	No
[82]	1	SP	2D Henon-Sine map	Pixel-wise scrambling, DNA encoding/decoding, DNA XOR	Yes
[58]	1	PS	Combination of Tent, Sine maps and Logistic, Sine maps	Scrambling, XOR	Yes
[112]	1	S	Elliptic curve, affine Hill cipher	Matrix multiplication under modulo 256	No
[73]	1	PPS	2D Logistic-adjusted-Sine map, Arnold transformation	Lookup table	No
[74]	1	PPSS	2D-SCMCI hyperchaotic map	Pixel-wise scrambling, modular addition	No
[93]	1	SS	LFSR, dynamic compound chaotic map	XOR, modular addition	No
[94]	1	PSPS	3D Latin square, Logistic map	Inter-pixel and intra-pixel scrambling, shifting, XOR	Yes
[75]	1	PS	Arnold's cat map, Chen's map	Pixel-wise scrambling, XOR	No
[89]	1	SP	Piece-wise linear chaotic map, Hill cipher	Matrix multiplication and matrix addition under modulo 256	No
[95]	1	S	Genetic algorithm, chaotic map, pseudo-random bit sequence generator	Mutation, Crossover, XOR, flipping	No
[76]	1	$(PS)^3$	2D-modified Henon map, hybrid chaotic shift transform	XOR, shifting, pixel-wise scrambling	No
[111]	1	PSP	Logistic map, Latin cubes	Pixel-wise scrambling, XOR	No

Table 7 continued

Ref. of scheme	No. of round	Structure	Mathematical primitive/ chaos map used	Operations used during encryption	Plaintext-sensitive key used (yes/no)
[96]	1	SP	S-box, enhanced Sine map, enhanced Logistic map	Pixel-wise scrambling, XOR	No

(DNA- Deoxyribonucleic Acid; LFSR- Linear Feedback Shift Register; PPS- Permutation-Permutation-Substitution; PPSS- Permutation-Permutation-Substitution-Substitution; PS- Permutation-Substitution; $(PS)^3$- Permutation-Substitution performed consecutively three times; PSP- Permutation-Substitution-Permutation; PSPS- Permutation-Substitution-Permutation-Substitution; PSS- Permutation-Substitution-Substitution; S- Substitution; SCMCI- Sine Cascade Modulation Couple Iterative; SP- Substitution-Permutation; SPS- Substitution-Permutation-Substitution; SS- Substitution-Substitution; XOR- Exclusive OR)

for schemes employing single or small (and fixed) number of rounds.

e For the resistance against chosen/known plaintext/ciphertext attacks many of the schemes, nowadays, utilise plaintext sensitivity in key-stream(s) generation. As per conventional symmetric encryption, the key should be plaintext-independent [1, 104]. Hence, relying security on plaintext-sensitive keys is debatable. Also, there is extra plaintext-specific information which is required to be communicated to the receiver for decryption, which is an extra overhead and hence should be avoided. The design of schemes and mathematical operations themselves should provide proper confusion and diffusion properties without reliance on plaintext-sensitive keys.

f Further, it is observed that despite efforts to use plaintext-sensitive keys as a countermeasure against chosen-plaintext attacks, some of such encryption schemes have been cryptanalysed successfully. It implies that the plaintext-sensitivity, if used, should be used appropriately.

g Also, many encryption schemes in their original forms appear to involve complex substitution/permutation operations, but they were easily reducible to simpler equivalent forms. These equivalent forms are then prone to cryptanalysis.

h Some authors have proposed use of multiple consecutive permutation and/or multiple consecutive substitution operations performed during each round to claim higher strength. However, their cryptanalysis reveal that such use of multiple substitution/permutation operations only adds to computational expense and do not add to the security of the encryption process because many a times such designs are reducible to equivalents with single permutation and/or substitution operation.

i Some researchers have explored use of other mathematical primitives with/without chaos, like DNA encoding/decoding. However, it is observed that including such encodings in the encryption process do not effectively add any security or enhance the confusion and diffusion properties, unless it is intertwined with thoughtfully designed operations. Additionally, while such incorporation (like DNA encoding) during encryption might apparently seem novel, but it need not necessarily make the encryption process stronger and remain as an unnecessary superficial add-on adding just to computational expense and not security.

j The authors of most of the original image encryption schemes under study, did not consider and discuss the resistance of their proposed schemes against popular attacks like brute-force attack, known/chosen-plaintext attack, chosen-ciphertext attack etc. which makes the security analysis of such schemes incomplete.

For better understanding, we outline the weaknesses observed in the cryptanalysed image encryption schemes in Fig. 11.

4.2 Suggestions for image encryption scheme designs

Following are our suggestions aimed at avoiding potential vulnerabilities or weaknesses in future designs of image encryption schemes. These suggestions offer valuable insight for designing more robust schemes that can resist cryptanalysis.

Table 8 Details of cryptanalytic attacks

Ref. of original scheme	Ref. of cryptanalytic attack	Type(s) of attack(s)	Scheme reduced to equivalent for attack (yes/no)	No. of plaintext-ciphertext pairs required for attack
[57]	[35]	Chosen-plaintext, chosen-ciphertext	Yes	$1 + log_L(mn), 1 + log_L(mn)$
[57]	[36]	Chosen-plaintext	Yes	$O(log_L(mn))$
[59]	[37]	Chosen-plaintext	No	$9 + \lceil(log_{256}m)\rceil + \lceil(log_{256}n)\rceil$
[60]	[38]	Chosen-plaintext	Yes	3
[61]	[39]	Chosen-plaintext	No	$O(3 + log_2(mn))$
[61]	[40]	Chosen-plaintext	No	2
[85]	[98]	Chosen-plaintext	No	3
[97]	[110]	Chosen-plaintext, known-plaintext	Yes	$\lceil 2\ log_{256}(mn)\rceil + 1$, 1
[87]	[86]	Chosen-plaintext	Yes	17
[77]	[41]	Chosen-plaintext	Yes	$\lceil \frac{mn}{BS^2 \times 256^{BS \times BS}} \rceil + 1$
[90]	[99]	Chosen-plaintext	No	5
[78]	[42]	Chosen-plaintext	No	$(mn/8) + 1$
[84]	[100]	Chosen-plaintext, known-plaintext, chosen-ciphertext	No	1, 1, 1
[62]	[43]	Chosen-plaintext	No	$O(L^2)$
[91]	[101]	Two methods of chosen-plaintext	Yes	3, 258
[63]	[44]	Chosen-plaintext	No	3
[64]	[45]	Chosen-plaintext	No	$O(\lceil log_2(m \times 24n)\rceil + 1)$
[65]	[46]	Chosen-plaintext followed by brute-force	Yes	10
[80]	[47]	Two chosen-plaintext	Yes	$\lceil log_2(mn)\rceil + 1$, $\lceil log_{256}(mn)\rceil + 1$
[66]	[48]	Chosen-plaintext, differential	No	1, 2
[67]	[49]	Chosen-plaintext, chosen-ciphertext	No	1, 1
[68]	[50]	Chosen-plaintext	No	$1 + \lceil log_L(mn)\rceil$
[69]	[21]	Chosen-plaintext	No	$O(log_L(mn))$
[70]	[21]	Chosen-plaintext	No	$O(n(mn)^2)$
[71]	[51]	Chosen-plaintext	Yes	$O(mn)$
[72]	[102]	Known-plaintext, chosen-plaintext	No	1, 2
[92]	[20]	Chosen-plaintext	No	2
[79]	[52]	Chosen-plaintext	Yes	$mn + 1$
[83]	[103]	Chosen-plaintext	Yes	$2 \times (mn \times 8) + 1$
[82]	[104]	Chosen-plaintext	Yes	$L + 255$
[58]	[53]	Chosen-plaintext	Yes	$\lceil(3mn/255)\rceil + 1$

Table 9 Weaknesses of cryptanalysed schemes and suggestions proposed by corresponding cryptanalysts

Ref. for original scheme	Weaknesses highlighted by corresponding cryptanalyst	Ref. for cryptanalytic attack	Suggested improvements to prevent cryptanalysis by corresponding cryptanalyst
[57]	Weak diffusion, and the keys are independent of plaintext.	[35]	To add plaintext-sensitivity to the key-stream using a hash value or hamming distance of plaintext, Also, cryptanalysts suggested using multiple rounds of encryption for better confusion/diffusion properties. Some random values can be added during encryption to improve security.
[57]	The cryptanalysts remarked that the keys are independent of plaintext. Also, poor operations are used, due to which the encryption scheme is reduced to an equivalent scheme for cryptanalysis.	[36]	To avoid the use of multiple consecutive permutation/diffusion operations and to give careful attention to designing the complex operations employed in the scheme.
[59]	The cryptanalysts remarked that the use of few plaintext independent key sequences as a weakness.	[37]	The cryptanalysts suggested introducing plaintext-sensitivity in the diffusion key-stream.
[60]	The use of the sum of pixels in a plain image as sensitivity, which is not unique to a plain image, and the lack of diffusion property.	[38]	To use plaintext-sensitivity in key-streams unpredictably and to give more attention to scheme design.
[61]	Both chaotic maps have periodic windows, which reduce key-space, and key-streams are not sensitive enough to plain images.	[39]	To avoid the existence of an equivalent key, to use complex operations for the proper diffusion/confusion properties, and to perform multiple encryption rounds, an appropriate chaotic system with robust chaos should be used to generate chaotic key-streams.
[61]	The cryptanalysts remarked that the key-streams being plaintext-independent is a weakness. Other weaknesses include the use of only the XOR operation for diffusion, and also the used permutation and substitution operations in the scheme are not intricate, hence, they are vulnerable to attack independently from one another (by the divide and conquer method).	[40]	To use different sets of key sequences to encrypt different images (i.e., to use plaintext-sensitive key-streams).
[85]	Lack of confusion and diffusion properties.	[98]	To avoid the consecutive use of operations like multiplication and XOR, which are invariant when applied to data comprising of all-zero's or one's, instead use these in combination with other substitution and permutation operations to offer resistance against chosen-plaintext attacks.
[97]	There are weak-keys in the scheme, and no key-space analysis is done. Also, the period of the Lucas series used in encryption is small.	[110]	To give extra attention while using the Lucas series for image encryption.

Table 9 continued

Ref. for original scheme	Weaknesses highlighted by corresponding cryptanalyst	Ref. for cryptanalytic attack	Suggested improvements to prevent cryptanalysis by corresponding cryptanalyst
[87]	Multiple consecutive diffusion operations provide security equivalent to a single diffusion operation only, hence decreasing the efficiency. Also, the sum of the pixels of a plain image is used for sensitivity, which is not unique to a plain image and makes the scheme vulnerable to chosen-plaintext attack.	[86]	To use intricate operations and to avoid using such operations, which only decrease efficiency rather than provide security, to use plaintext-sensitivity in key-stream, which is unique to a plain image, and also to use both binary and unary diffusion operations for proper diffusion properties.
[77]	Scheme design is weak, and poor confusion and diffusion properties lead to attacks. Only XOR is used for diffusion, which reveals one-to-one relationships between keys and ciphertext. Secret keys are plaintext-independent, and scrambling and diffusion operations are independent of each other, so they can be cryptanalyzed independently of one another.	[41]	To use a hyperchaotic map with better chaos, to use more intricate operations, and to use plaintext-sensitivity in key-stream. which is unique to a plain image.
[90]	Lack of diffusion property.	[99]	To use plaintext-sensitive key-streams for adequate security.
[78]	The existence of a linear relationship between the plain image and the cipher image and bad randomness in the key-stream lead to cryptanalysis	[42]	To use nonlinear operations, use modular operations between permuted images and a random matrix to increase security by increasing computational complexity
[84]	Only a single round of XOR is used for diffusion, which leads to poor security	[100]	To introduce more rounds and operations to enhance the security of the scheme, plaintext-sensitive key-streams should be used to avoid chosen-plaintext attacks
[62]	Plaintext-sensitivity relies only on the average intensity of the plain image, key-space is not large enough	[43]	To use the hash value of a plain image as plaintext-sensitivity in the key-stream to mitigate a chosen-plaintext attack, which is unique to a plain image.
[91]	A single round is used, lack of diffusion property	[101]	To use strong correlation between the keys and the plaintext, to perform multiple rounds, to use nonlinear substitution, and to design a more intricate diffusion step
[63]	Only XOR is used for diffusion; less intricate operations and single-round encryption are used, providing poor security	[44]	To use more intricate operations for better confusion/diffusion properties
[64]	A plain linear-nonlinear-linear structure makes the scheme prone to a chosen-plaintext attack	[45]	To use dynamic keys that vary with the plain image or time, as well as to use multiple rounds and more efficient diffusion operations
[65]	Lack of confusion and diffusion properties; multiple consecutive permutation operations provide strength equivalent to a single permutation operation only; single round and weak plaintext-sensitivity are used	[46]	Not suggested

Table 9 continued

Ref. for original scheme	Weaknesses highlighted by corresponding cryptanalyst	Ref. for cryptanalytic attack	Suggested improvements to prevent cryptanalysis by corresponding cryptanalyst
[80]	The cryptanalysts remarked that the use of the same key sequences (plaintext-independent key) for encrypting all plain images as a weakness	[47]	To use high correlation between the key and the plaintext and to add a nonlinear substitution phase, to add an efficient random block for better diffusion
[66]	The cryptanalysts remarked use of the same key-stream for encrypting multiple blocks of plaintext as a weakness. Also, use of row-wise and column-wise permutation instead of complex pixel-wise permutation as another weakness. They also questioned the use of only XOR during substitution and observed that the used chaotic map is not desirably robust	[48]	To use pixel-level permutation instead of row- and column-level permutation, to employ a chaotic map with robust chaotic properties, to use an appropriate block-cipher mode like CBC (Cipher Block Chaining) mode while encrypting different plaintext blocks
[67]	Only the confusion property is used, and the structure of the scheme is very simple	[49]	To add a permutation step along with substitution for better confusion/diffusion properties
[68]	Simple structure is used, lack of confusion/diffusion	[50]	To add plaintext-sensitivity to the key-stream, to add substitution before diffusion operation, and to improve the scheme's design for better security
[69]	Lack of confusion property, poor diffusion	[21]	To perform two compulsory tests- all-zero and unit image and to assess the resistance against standard cryptographic attacks during scheme design
[70]	The average sum of the pixels in a plain image is used as sensitivity, which is not unique to a plain image; a small key-space is used	[21]	To use a key of at least 128 bits to avoid brute-force attacks, to use plaintext-sensitivity in the key-stream carefully, which is unique to a plain image
[71]	Two consecutive diffusion operations provide strength equivalent to a single diffusion operation, resulting in poor diffusion and a decrease in efficiency	[51]	To use plaintext-sensitive keys, use multiple types of operations (like both modular addition and XOR operations) instead of just one, i.e., modular addition, during diffusion
[72]	Poor diffusion, the algorithm can only apply to square images, the XOR operation simply operates on the corresponding bit plane (one-to-one map)	[102]	To make an algorithm suitable for an image of any dimension, one pixel of a plain image should contribute to many pixels of a cipher image
[92]	The grey values of nine specific pixels do not change during diffusion; the permutation process is weak	[20]	To use plaintext-sensitivity in the key-streams carefully
[79]	The effective key-space is smaller than the claimed key-space by the author of the original scheme due to presence of multiple equivalent secret keys, lack of diffusion property	[52]	The cryptanalysts suggested the use of an appropriate mechanism to generate chaotic system parameters from the initial key in order to avoid the presence of multiple keys. Also, they suggested to avoid excess random pixel insertions to mitigate the communication overhead, and to use the hash value of a plain image for the key-stream generation to avoid a chosen-plaintext attack

Table 9 continued

Ref. for original scheme	Weaknesses highlighted by corresponding cryptanalyst	Ref. for cryptanalytic attack	Suggested improvements to prevent cryptanalysis by corresponding cryptanalyst
[83]	Weak confusion and diffusion properties, there are a large number of equivalent secret keys in the key-space.	[103]	To introduce the hash value of the plain image for key-stream generation and to evaluate the newly designed encryption scheme from the perspective of cryptanalysts
[82]	An S-box is equivalent to DNA random coding and XOR operations, which makes cryptanalysis easy.	[104]	To use self-adaptive recoverable plaintext-sensitivity in the key-stream utilised during the per-round operations
[58]	The cryptanalyst remarked on the flawed definition of the chaotic system used. Even the corrected chaotic system is identified as weak. The recovery of a plain image to a certain degree of visibility from a noise-added ciphertext acts as a vulnerability for a chosen-ciphertext attack	[53]	To avoid the use of consecutive similar operations as they do not provide proper security, use modular addition in place of XOR to combine the different chaotic maps as it generates a more suitable map
[112]	Weak confusion property, use of smaller key-space	[22]	To include proper confusion and diffusion properties and to use large key- spaces to resist brute-force attacks
[73]	The keystream is fixed for the operations; the entropy used for plaintext-sensitivity in the key-stream remains unchanged, which leads to a chosen-plaintext attack	[19]	To introduce the hash value of plain images as plaintext-sensitivity in key-stream generation. Improvement in compression mechanism is also suggested, though beyond the scope of this review
[74]	Poorly designed operations and multiple consecutive permutation/substitution operations provide the strength of a single permutation/substitution operation	[54]	To introduce plaintext-sensitivity in the key-stream, to use large key-spaces and intricate operations, and also to use multiple rounds of encryption.
[93]	Weak keys, poor encryption design, and keys that are not plaintext-sensitive.	[105]	Not suggested
[94]	The diffusion step can not resist differential attack, the use of plaintext-sensitivity is deterministic.	[106]	To assess the scheme against well-known attacks rather than only statistical tests, to avoid weak and invalid keys in the encryption scheme, to use nonlinear and complex diffusion, and to use irreversible encryption design without any key
[75]	Shuffling is weak, hence poor diffusion.	[56]	To use plaintext-sensitive key-streams carefully
[89]	There is a linear relationship between plaintext and ciphertext, which leads to cryptanalysis	[88]	To strengthen the scheme against an all-zero plain image attack by introducing an extra matrix operation
[95]	Weak diffusion property	[107]	Not suggested.
[76]	Two consecutive diffusion operations provide the strength of one diffusion operation.	[55]	To use different initial values for different primitives, use plaintext-sensitive key-streams to resist chosen-plaintext attacks.
[111]	The generation of the Latin cube is independent of the plain image, so different chosen-plain images can produce the same key-streams. The diffusion step is too simple, which leads to a lack of security.	[108]	To enhance the plaintext-sensitivity in key-streams, to increase the number of rounds of operations, and to use a more complex diffusion step for proper security
[96]	Only 24-bit keys provide security instead of 128-bit keys due to weak keys	[109]	Not suggested

(XOR- Exclusive OR)

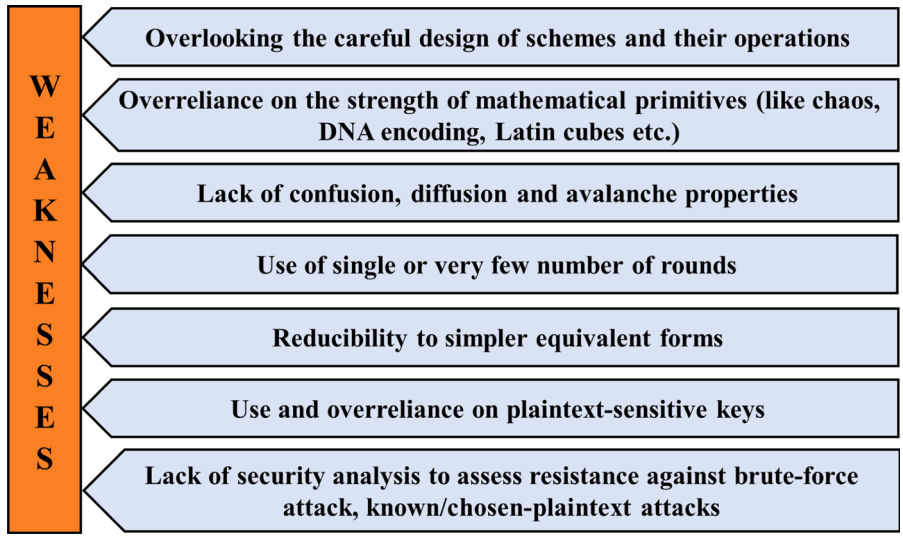


Fig. 11 Findings on weak designs in image encryption schemes

- ✓ It is crucial to employ carefully designed operations which are not only superficially complex but add to the overall security. Every operation and mathematical primitive should add to the proper confusion and/or diffusion property.
- ✓ Overreliance on properties of chaos without careful design of the encryption schemes and their operations should be avoided.
- ✓ Overreliance on plaintext-sensitivity of keys should be avoided. Further, it is highlighted that plaintext-sensitivity adds unnecessary overhead during communication of the key and hence, it should anyways be avoided. Also, traditionally, the encryption key is defined to be independent of the plaintext [1,104].
- ✓ Though discouraged, however, under any circumstance, if the scheme designer still chooses to use plaintext-sensitivity for keys, it should be used in an adequate manner so that plaintext information used to provide sensitivity changes apparently randomly with any change in the plaintext. That is, such chosen plaintexts should not be easily identifiable which would contribute same plaintext-sensitivity to the key as the original plaintext (being attacked). Like, use of hash value of the plain image would be better than sum of its pixel values for offering plaintext-sensitivity.
- ✓ A small number of rounds and the use of multiple consecutive permutations and/or multiple consecutive substitutions should be avoided. This is because encryption designs based on such approaches are easily reducible to equivalent simpler forms that are then easier to break. Also, such approaches decrease efficiency without adding much to the security.
- ✓ The design of the permutation and substitution operations of the scheme should ensure that each cipher image pixel receives contribution from multiple plain image pixels and key-stream bytes, so as to resist one of the most widely used chosen-plaintext attacks like the one with all-black chosen image. In short, the relationship between cipher image pixels with the plain image pixels and the key-stream bytes should be non-linear and sufficiently complex.
- ✓ Ensuring the scheme exhibits the avalanche property is also crucial to ascertain that the scheme possesses effective confusion and diffusion properties. Additionally, performing thorough efficiency and security analysis is of utmost importance to balance the computational performance and strength of schemes.
- ✓ The scheme designers should also ensure and demonstrate resistance of the proposed schemes against well-known attacks like brute-force attack, known/chosen-plaintext attack, chosen-ciphertext attack etc. as part of the security analysis itself.

On the basis of the above-mentioned suggestions, we provide a checklist of guidelines (Table 10) which can be followed by researchers while designing new image encryption schemes in future. This would help the future schemes to not carry the same weaknesses as identified in existing cryptanalysed schemes (Sect. 4.1).

Table 10 Checklist of guidelines for image encryption scheme design

S. No.	Recommended	Do	Don't
1	Careful design of operations	✓	
2	Use of single or very few number of rounds		✓
3	Use of multiple consecutive permutation and/or multiple consecutive substitution operations in per-round operation		✓
4	Overreliance on strength of mathematical primitives (like chaos etc.)		✓
5	Use of plaintext-sensitive key		✓
6	Perform avalanche property analysis for effective confusion and diffusion properties	✓	
7	Assess resistance against known/chosen-plaintext attack	✓	

5 Limitations

While we attempted to provide a comprehensive review but there have been few limitations as well. This review incorporated all relevant articles from Web of Science and Scopus published during 2019–23. Other databases like ACM and IEEE Xplore were also searched, but since mostly duplicate articles were identified, hence, the articles from these databases were entirely skipped. That is, manual shortlisting of every article was not carried out for search results obtained on ACM and IEEE Xplore. Also, though it has been a conscious effort to present our findings and observations objectively, despite every effort to avoid it, there could still be some personal and confirmation biases involved.

6 Conclusion

This paper provides an extensive review of cryptanalytic attacks on the image encryption schemes published during 2019–23. Analysis shows that lightweight applications often face a trade-off between efficiency and security. The number of rounds in the encryption schemes should not be very small, and it should be appropriate in accordance with the per-round operations used, so as to balance the security and efficiency aspects. Also, the undue heavy reliance on plaintext-sensitive keys/chaos to provide security without thoughtful design raises concerns about the robustness of such cryptographic schemes. Though discouraged, even if plaintext-sensitive keys are used, the plaintext-related information should be such that identifying chosen plaintexts offering the same plaintext-sensitivity should not be possible, so that the corresponding key-streams generated should not be the same. Finally, security should not solely depend on the plaintext-sensitive nature of the key, and a holistic approach to encryption scheme design is essential. This paper provides valuable insights for researchers to consider in future work, especially in designing more robust image encryption schemes and devising methods to attack the existing ones. Essentially, this review offers a comprehensive resource for researchers interested in strengthening encryption methods and for those looking to cryptanalyse and uncover vulnerabilities in the existing schemes.

Acknowledgements The authors are thankful to the anonymous reviewers for their valuable suggestions which greatly improved the quality and presentation of this review paper. The second author is thankful to the Department of Science and Technology (DST), Government of India, for providing DST-INSPIRE fellowship (Inspire code- IF220144).

Author contributions S.D. did conceptualization of the manuscript. Both S.D. and K.Y. did literature search, analysis, draft writing and its editing. S.D. reviewed and revised the first draft. Both the authors revised the manuscript to incorporate reviewers' suggestions during the review process. All authors reviewed the final manuscript and approved the same.

Funding Not applicable.

Data Availability Statement The data for this paper is available in the public domain accessible freely or on subscription basis.

Declarations

Materials availability Not applicable.

Code availability Not applicable.

Conflict of interest All the authors declare no conflict of interest.

Ethics approval and consent to participate Not applicable.

Consent for publication Not applicable.

References

1. Stallings, W.: Cryptography and Network Security: Principles and Practice. Pearson Education, London (2003)
2. Daemen, J., Rijmen, V.: Aes proposal: Rijndael (1999)
3. Aumasson, J.-P.: Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, San Francisco (2017)
4. Devaney, R.: An Introduction to Chaotic Dynamical Systems. CRC Press, Boca Raton (2018)
5. Sprott, J.C.: Chaos and Time-Series Analysis. Oxford University Press Inc, Oxford (2003)
6. Ayubi, P., Setayeshi, S., Rahmani, A.M.: Chaotic complex hashing: a simple chaotic keyed hash function based on complex quadratic map. Chaos Solitons I Fractals **173**, 113647 (2023). https://doi.org/10.1016/j.chaos.2023.113647
7. Wolf, A., Swift, J.B., Swinney, H.L., Vastano, J.A.: Determining Lyapunov exponents from a time series. Physica D: Nonlinear Phenomena **16**(3), 285–317 (1985). https://doi.org/10.1016/0167-2789(85)90011-9
8. Steven, S.: Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering. Westview Press, Boulder (2015)
9. Frigg, R.: In what sense is the Kolmogorov–Sinai entropy a measure for chaotic behaviour? Bridging the gap between dynamical systems theory and communication theory. Br. J. Philos. Sci. (2004). https://doi.org/10.1093/bjps/55.3.411
10. Paul, B., Trivedi, G.: Post quantum cryptography algorithms: a review and applications. In: International Conference on Intelligent Technologies, pp. 3–17. Springer (2022)
11. May, R.M.: Simple mathematical models with very complicated dynamics. Nature **261**(5560), 459–467 (1976)
12. Crampin, M., Heal, B.: On the chaotic behaviour of the tent map. Teach. Math. Appl.: Int. J. IMA **13**(2), 83–89 (1994)
13. Arnold, V.I., Avez, A.: Ergodic Problems of Classical Mechanics. W.A. Benjamin Inc, San Francisco (1968)
14. Schack, R., Caves, C.M.: Information and entropy in the Baker's map. Phys. Rev. Lett. **69**(23), 3413 (1992)
15. Khan, M., Asghar, Z.: A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and s 8 permutation. Neural Comput. Appl. **29**, 993–999 (2018)
16. Curry, J.H.: A generalized Lorenz system. Commun. Math. Phys. **60**, 193–204 (1978)
17. Letellier, C., Dutertre, P., Maheu, B.: Unstable periodic orbits and templates of the Rössler system: toward a systematic topological characterization. Chaos: Interdiscip. J. Nonlinear Sci. **5**(1), 271–282 (1995)
18. Mehmood, A., Shafique, A., Alawida, M., Khan, A.N.: Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques. IEEE Access **12**, 27530–27555 (2024)
19. Xiang, Y., Xiao, D., Zhang, R., Liang, J., Liu, R.: Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer. Inform. Sci. **545**, 188–206 (2021)
20. Liu, L., Zhang, Z., Chen, R.: Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos. IEEE Access **7**, 126450–126463 (2019)
21. Mastan, J.M.K., Pandian, R.: Cryptanalysis of two similar chaos-based image encryption schemes. Cryptologia **45**(6), 541–552 (2021)
22. Lone, P.N., Singh, D., Stoffová, V., Mishra, D.C., Mir, U.H., Kumar, N.: Cryptanalysis and improved image encryption scheme using elliptic curve and affine hill cipher. Mathematics **10**(20), 3878 (2022)
23. Heys, H.M.: A tutorial on linear and differential cryptanalysis. Cryptologia **26**(3), 189–221 (2002)
24. Li, C., Zhang, Y., Xie, E.Y.: When an attacker meets a cipher-image in 2018: A year in review. J. Inform. Secur. Appl. **48**, 102361 (2019)
25. Abba, A., Teh, J.S., Alawida, M.: Towards accurate keyspace analysis of chaos-based image ciphers. Multim. Tools Appl. 1–20 (2024)
26. Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., et al.: The prisma 2020 statement: an updated guideline for reporting systematic reviews. Bmj **372** (2021)
27. Alawida, M.: A novel chaos-based permutation for image encryption. J. King Saud Univ.-Comput. Inform. Sci. **35**(6), 101595 (2023)
28. Alawida, M.: Enhancing logistic chaotic map for improved cryptographic security in random number generation. J. Inform. Secur. Appl. **80**, 103685 (2024)
29. Singh, L.D., Thingbaijam, R., Patgiri, R., Singh, K.M.: Cryptanalysis of cross-coupled chaotic maps multi-image encryption scheme. J. Inform. Secur. Appl. **80**, 103694 (2024)
30. Wong, K.-W., Yap, W.-S., Goi, B.-M., Wong, D.C.-K., Ye, G.: Cryptanalysis of an image encryption scheme based on two-point diffusion strategy and Henon map. J. Inform. Secur. Appl. **81**, 103692 (2024)
31. Wen, H., Lin, Y., Feng, Z.: Cryptanalyzing a bit-level image encryption algorithm based on chaotic maps. Int. J. Eng. Sci. Technol. **51**, 101634 (2024)
32. Li, M., Wang, M., Fan, H., Liu, Y., Zhang, H., Nan, H.: On the security of image cryptosystems using drpe based on scrambling and diffusion. Opt. Quantum Electron. **56**(2), 241 (2024)
33. Islam, Y., Li, C., Sun, K., He, S.: Enhancing image security through an advanced chaotic system with free control and

zigzag scrambling encryption. Multim. Tools Appl. 1–29 (2024)
34. Qu, L., Li, M., Sun, Y., Su, S., Liu, Y., Zhang, L.: Security analysis of a reversible data hiding scheme in encrypted images by redundant space transfer. J. King Saud Univ.-Comput. Inform. Sci. **36**(1), 101914 (2024)
35. Zhang, C., Chen, J., Chen, D.: Cryptanalysis of an image encryption algorithm based on a 2d hyperchaotic map. Entropy **24**(11), 1551 (2022)
36. Jiang, Q., Yu, S., Wang, Q.: Cryptanalysis of an image encryption algorithm based on two-dimensional hyperchaotic map. Entropy **25**(3), 395 (2023)
37. Zhu, S., Zhu, C., Yan, H.: Cryptanalyzing and improving an image encryption algorithm based on chaotic dual scrambling of pixel position and bit. Entropy **25**(3), 400 (2023)
38. Lin, C.-Y., Wu, J.-L.: Cryptanalysis and improvement of a chaotic map-based image encryption system using both plaintext related permutation and diffusion. Entropy **22**(5), 589 (2020)
39. Wen, H., Yu, S.: Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. Eur. Phys. J. Plus **134**, 1–16 (2019)
40. Zhu, S., Zhu, C.: Security analysis and improvement of an image encryption cryptosystem based on bit plane extraction and multi chaos. Entropy **23**(5), 505 (2021)
41. Liu, Y., Qin, Z., Liao, X., Wu, J.: Cryptanalysis and enhancement of an image encryption scheme based on a 1-d coupled sine map. Nonlinear Dyn. **100**, 2917–2931 (2020)
42. Chen, Y., Tang, C., Ye, R.: Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. **167**, 107286 (2020)
43. Huang, R., Liao, X., Dong, A., Sun, S.: Cryptanalysis and security enhancement for a chaos-based color image encryption algorithm. Multim. Tools Appl. **79**, 27483–27509 (2020)
44. Dou, Y., Li, M.: Cryptanalysis of a new color image encryption using combination of the 1d chaotic map. Appl. Sci. **10**(6), 2187 (2020)
45. Li, M., Wang, P., Liu, Y., Fan, H.: Cryptanalysis of a novel bit-level color image encryption using improved 1d chaotic map. IEEE Access **7**, 145798–145806 (2019)
46. Mokhnache, A., Ziet, L.: Cryptanalysis of a pixel permutation based image encryption technique using chaotic map. Traitement du Signal **37**(1), 95–100 (2020)
47. Li, M., Wang, P., Yue, Y., Liu, Y.: Cryptanalysis of a secure image encryption scheme based on a novel 2d sine–cosine cross-chaotic map. J. Real-Time Image Process. 1–15 (2021)
48. El Hanouti, I., El Fadili, H., Zenkouar, K.: Cryptanalysis of an embedded systems' image encryption. Multim. Tools Appl. **80**(9), 13801–13820 (2021)
49. Alanazi, A.S., Munir, N., Khan, M., Asif, M., Hussain, I.: Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes. IEEE Access **9**, 93795–93802 (2021)
50. Li, M., Zhou, K., Ren, H., Fan, H.: Cryptanalysis of permutation-diffusion-based lightweight chaotic image encryption scheme using cpa. Appl. Sci. **9**(3), 494 (2019)
51. Chen, R., Liu, L., Zhang, Z.: Cryptanalysis on a permutation-rewriting-diffusion (prd) structure image encryption scheme. Multim. Tools Appl. **82**(3), 4289–4317 (2023)
52. Feng, W., He, Y., Li, H., Li, C.: Cryptanalysis and improvement of the image encryption scheme based on 2d logistic-adjusted-sine map. Ieee Access **7**, 12584–12597 (2019)
53. Zhang, Y.: Security analysis of a chaos triggered image encryption scheme. Multim. Tools Appl. **78**(22), 31303–31318 (2019)
54. Alshehri, M., Almakdi, S., Al Qathrady, M., Ahmad, J.: Cryptanalysis of 2d-scmci hyperchaotic map based image encryption algorithm. Comput. Syst. Sci. Eng. **46**(2), 2401–2414 (2023)
55. Zhou, K., Xu, M., Luo, J., Fan, H., Li, M.: Cryptanalyzing an image encryption based on a modified Henon map using hybrid chaotic shift transform. Digit. Signal Process. **93**, 115–127 (2019)
56. Mukherjee, P., Rarhi, K., Mishra, A., Bhattacharya, A.: Cryptanalysis of a chaotic key-based image encryption scheme. In: Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2018, Volume 3, pp. 165–173 (2019). Springer
57. Gao, X.: Image encryption algorithm based on 2d hyperchaotic map. Opt. Laser Technol. **142**, 107252 (2021)
58. Ramalingam, B., Ravichandran, D., Annadurai, A.A., Rengarajan, A., Rayappan, J.B.B.: Chaos triggered image encryption-a reconfigurable security solution. Multim. Tools Appl. **77**, 11669–11692 (2018)
59. Deng, X., Liao, C., Zhu, C., Chen, Z.: Image encryption algorithms based on chaos through dual scrambling of pixel position and bit. J. Commun. **35**(3), 216–223 (2014)
60. Huang, L., Cai, S., Xiao, M., Xiong, X.: A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion. Entropy **20**(7), 535 (2018)
61. Shafique, A., Shahid, J.: Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. Eur. Phys. J. Plus **133**(8), 331 (2018)
62. Wang, H., Xiao, D., Chen, X., Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map. Signal Process. **144**, 444–452 (2018)
63. Pak, C., Huang, L.: A new color image encryption using combination of the 1d chaotic map. Signal Process. **138**, 129–137 (2017)
64. Pak, C., An, K., Jang, P., Kim, J., Kim, S.: A novel bit-level color image encryption using improved 1d chaotic map. Multim. Tools Appl. **78**(9), 12027–12042 (2019)
65. Anwar, S., Meghana, S.: A pixel permutation based image encryption technique using chaotic map. Multim. Tools Appl. **78**, 27569–27590 (2019)
66. Lin, Z., Liu, J., Lian, J., Ma, Y., Zhang, X.: A novel fast image encryption algorithm for embedded systems. Multim. Tools Appl. **78**, 20511–20531 (2019)
67. Khan, M.: A novel image encryption scheme based on multiple chaotic s-boxes. Nonlinear Dyn. **82**(1–2), 527–533 (2015)
68. Mondal, B., Kumar, P., Singh, S.: A chaotic permutation and diffusion based image encryption algorithm for secure communications. Multim. Tools Appl. **77**, 31177–31198 (2018)

69. Beloucif, A., Noui, O., Noui, L.: Design of a tweakable image encryption algorithm using chaos-based schema. Int. J. Inform. Comput. Secur. **8**(3), 205–220 (2016)
70. 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 **7**, 74070–74080 (2019)
71. Ye, G., Pan, C., Huang, X., Mei, Q.: An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dyn. **94**, 745–756 (2018)
72. Shafique, A., Shahid, J.: Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. Eur. Phys. J. Plus **133**(8), 331 (2018)
73. Liu, Z.-L., Pun, C.-M.: Reversible data-hiding in encrypted images by redundant space transfer. Inform. Sci. **433**, 188–203 (2018)
74. Sun, J.: 2d-scmci hyperchaotic map for image encryption algorithm. Ieee Access **9**, 59313–59327 (2021)
75. Al-Maadeed, S., Al-Ali, A., Abdalla, T.: A new chaos-based image-encryption and compression algorithm. J. Electr. Comput. Eng. **2012**, 15–15 (2012)
76. Sheela, S., Suresh, K., Tandur, D.: Image encryption based on modified Henon map using hybrid chaotic shift transform. Multim. Tools Appl. **77**, 25223–25251 (2018)
77. Yosefnezhad Irani, B., Ayubi, P., Amani Jabalkandi, F., Yousefi Valandar, M., Jafari Barani, M.: Digital image scrambling based on a new one-dimensional coupled sine map. Nonlinear Dyn. **97**(4), 2693–2721 (2019)
78. Hua, Z., Yi, S., Zhou, Y.: Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. **144**, 134–144 (2018)
79. Hua, Z., Zhou, Y.: Image encryption using 2d logistic-adjusted-sine map. Inform. Sci. **339**, 237–253 (2016)
80. Mondal, B., Behera, P.K., Gangopadhyay, S.: A secure image encryption scheme based on a novel 2d sine-cosine cross-chaotic (sc3) map. J. Real-Time Image Process. **18**(1), 1–18 (2021)
81. Chen, J.-X., Zhu, Z.-L., Fu, C., Zhang, L.-B., Zhang, Y.: An efficient image encryption scheme using lookup table-based confusion and diffusion. Nonlinear Dyn. **81**, 1151–1166 (2015)
82. Wu, J., Liao, X., Yang, B.: Image encryption using 2d hénon-sine map and dna approach. Signal Process. **153**, 11–23 (2018)
83. Wu, J., Shi, J., Li, T.: A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and dna-level diffusion. Entropy **22**(1), 5 (2019)
84. Khan, M., Masood, F., Alghafis, A., Amin, M., Batool Naqvi, S.I.: A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and brownian motion. PLoS ONE **14**(12), 0225031 (2019)
85. Masood, F., Ahmad, J., Shah, S.A., Jamal, S.S., Hussain, I.: A novel hybrid secure image encryption based on Julia set of fractals and 3d Lorenz chaotic map. Entropy **22**(3), 274 (2020)
86. Panwar, K., Purwar, R.K., Jain, A.: Cryptanalysis and improvement of a color image encryption scheme based on dna sequences and multiple 1d chaotic maps. Int. J. Bifur. Chaos **29**(08), 1950103 (2019)
87. Wu, X., Kan, H., Kurths, J.: A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps. Appl. Soft Comput. **37**, 24–39 (2015)
88. Kumar, V.N., Ravi Shankar, N.: Cryptanalysis of a new cryptosystem of color image using a dynamic-chaos hill cipher algorithm: A chosen ciphertext attack. In: Progress in Computing, Analytics and Networking: Proceedings of ICCAN 2019, pp. 475–482. Springer (2020)
89. Hraoui, S., Gmira, F., Abbou, M.F., Oulidi, A.J., Jarjar, A.: A new cryptosystem of color image using a dynamic-chaos hill cipher algorithm. Procedia Comput. Sci. **148**, 399–408 (2019)
90. Deb, S., Biswas, B., Bhuyan, B.: Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field. Multim. Tools Appl. **78**, 34901–34925 (2019)
91. Khan, M., Masood, F.: A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multim. Tools Appl. **78**, 26203–26222 (2019)
92. Li, Z., Peng, C., Li, L., Zhu, X.: A novel plaintext-related image encryption scheme using hyper-chaotic system. Nonlinear Dyn. **94**, 1319–1333 (2018)
93. Tong, X.-j: The novel bilateral-diffusion image encryption algorithm with dynamical compound chaos. J. Syst. Softw. **85**(4), 850–858 (2012)
94. Hu, G., Xiao, D., Zhang, Y., Xiang, T.: An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy. Nonlinear Dyn. **87**, 1359–1375 (2017)
95. Biswas, K., Muthukkumarasamy, V., Singh, K.: An encryption scheme using chaotic map and genetic operations for wireless sensor networks. IEEE Sensors J. **15**(5), 2801–2809 (2014)
96. ESSAID, M., AKHARRAZ, I., SAAIDI, A., MOUHIB, A.: A new approach of image encryption based on dynamic substitution and diffusion operations. In: 2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS), pp. 1–6. IEEE (2019)
97. Batool, S.I., Waseem, H.M.: A novel image encryption scheme based on Arnold scrambling and Lucas series. Multim. Tools Appl. **78**, 27611–27637 (2019)
98. Munir, N., Khan, M., Jamal, S.S., Hazzazi, M.M., Hussain, I.: Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map. Math. Comput. Simul. **190**, 826–836 (2021)
99. Arora, A., Sharma, R.K.: Cryptanalysis and enhancement of image encryption scheme based on word-oriented feed back shift register. Multim. Tools Appl. **81**(12), 16679–16705 (2022)
100. Munir, N., Khan, M., Al Karim Haj Ismail, A., Hussain, I.: Cryptanalysis and improvement of novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. Multim. Tools Appl. **81**(5), 6571–6584 (2022)
101. Fan, H., Zhang, C., Lu, H., Li, M., Liu, Y.: Cryptanalysis of a new chaotic image encryption technique based on multiple discrete dynamical maps. Entropy **23**(12), 1581 (2021)
102. 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 **7**, 74070–74080 (2019)
103. Feng, W., Zhang, J.: Cryptanalzing a novel hyper-chaotic image encryption scheme based on pixel-level filtering and dna-level diffusion. IEEE Access **8**, 209471–209482 (2020)
104. Chen, J., Chen, L., Zhou, Y.: Cryptanalysis of a dna-based image encryption scheme. Inform. Sci. **520**, 130–141 (2020)
105. Alshammari, B.: Cryptanalysis of a bilateral-diffusion image encryption algorithm based on dynamical compound chaos. Przeglad Elektrotechniczny **1**(1), 130–133 (2021)
106. Chen, L., Chen, J., Ma, L., Wang, S.: Cryptanalysis of a chaotic image cipher based on plaintext-related permutation and lookup table. Nonlinear Dyn. **100**(4), 3959–3978 (2020)
107. Wong, K.-W., Yap, W.-S., Wong, D.C.-K., Phan, R.C.-W., Goi, B.-M.: Cryptanalysis of genetic algorithm-based encryption scheme. Multim. Tools Appl. **79**, 25259–25276 (2020)
108. Zhang, Z., Yu, S.: On the security of a Latin-bit cube-based image chaotic encryption algorithm. Entropy **21**(9), 888 (2019)
109. Teseleanu, G.: Security analysis of a color image encryption scheme based on dynamic substitution and diffusion operations. Cryptology ePrint Archive (2022)
110. El Hanouti, I., El Fadili, H., Zenkouar, K.: Breaking an image encryption scheme based on Arnold map and Lucas series. Multim. Tools Appl. **80**(4), 4975–4997 (2021)
111. Xu, M., Tian, Z.: A novel image cipher based on 3d bit matrix and Latin cubes. Inform. Sci. **478**, 1–14 (2019)
112. Dawahdeh, Z.E., Yaakob, S.N., Othman, R.R.: A new image encryption technique combining elliptic curve cryptosystem with hill cipher. J. King Saud Univ.-Comput. Inform. Sci. **30**(3), 349–355 (2018)