Differential Cryptanalysis on Chaotic Based Image Encryption Scheme

To cite this article: K W Wong *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **495** 012041

Differential Cryptanalysis on Chaotic Based Image Encryption Scheme

K W Wong, W S Yap, B M Goi, Denis C K Wong

Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, 43000 Kajang, Selangor, Malaysia

E-mail: wongkw@utar.edu.my

Abstract. Image encryption schemes based on chaotic maps and systems have been investigated for more than one decade. However, many proposed schemes that obtained good score in the statistical tests, i.e. number of pixel changing rate and unified average changed intensity were proven to be insecure against differential cryptanalysis. Differential cryptanalysis is a chosen plaintext attack that utilizes the high probabilities of occurrence of a specific plaintext-ciphertext difference. In this paper, we present the weaknesses of these image encryption schemes against differential cryptanalysis and discuss how a cryptanalyst can exploit them to demonstrate the security deficiency of the schemes.

1. Introduction

The rapid development of computer network technology allows widespread transmission of multimedia data such as images and videos over insecure communication channels. Therefore, a fast and secure image encryption method is deemed important to protect the multimedia data from being accessed by the unauthorized users. The traditional data encryption methods such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) are no longer suitable for image encryption due to the bulk data capacity and high data capacity. To overcome this drawback, different image encryption methods were proposed based on DNA [1,2], hash function [3], Substitution-box (S-box) [4] and chaotic maps [5–13].

In recent years, chaotic based image encryption becomes a main focal of research in the information and communication security field. Chaos can fulfil the requirement of designing a fast and efficient encryption scheme due to its inherent characteristics, such as aperiodicity, very sensitive on the initial conditions and system parameters, ergodicity and random-like behaviours. Therefore, chaos is widely used in building the permutation matrices, generating a pseudorandom bit sequence which is useful in performing some basic encryption operations, and producing the ciphertext directly when the elements of plaintext are used as the control parameters or initial conditions of the chaotic systems [14]. Many image encryption schemes designed based on chaotic maps and systems have been proposed [5–13]. These schemes were claimed to be safe against differential cryptanalysis because they obtained a good score in the number of pixel change rate and unified average change intensity, which are two statistical/quantitative tests that ensure the strength of the underlying encryption algorithm against differential attack.

Differential cryptanalysis was first introduced by Biham and Shamir in 1991 [15]. This attack is primarily designed to attack the block cipher but its application has been extended also to stream ciphers

Published under licence by IOP Publishing Ltd

and cryptographic hash functions [16–18]. There are some variants that generalized from differential cryptanalysis. One of the most significant variants is impossible differential cryptanalysis. The ideology of this technique was first started by Knudsen [19] to attack DEAL block cipher and later formalized and named it as impossible differential cryptanalysis by Biham *et al.* [20]. The other variants of differential cryptanalysis include boomerang attack [21], amplified boomerang attack [22] and rectangle attack [23]. Since computation efficiency of differential attack is much better than brute force attack, therefore both differential cryptanalysis and impossible differential cryptanalysis have been applied to the current image encryption schemes. The vulnerability of existing schemes to differential cryptanalysis has shown that the statistical tests are insufficient to ensure the security of an encryption algorithm [14,24–31].

In this paper, we present the pitfalls and drawbacks that commonly found in the chaotic based image encryption schemes which can help the designer to propose an encryption algorithm that is secure from the differential-like attacks. The differential cryptanalytic approaches that applied on the encryption schemes have been revisited and compared. From the survey, it was found that the encryption algorithms shared some common characteristics which could allow a cryptanalyst to recover the information of secret key with lower time complexity as compared to brute-force attack. The design that is vulnerable to differential cryptanalysis has been highlighted.

The outline of this paper is organized as follow. Section II introduces the preliminaries of the differential cryptanalysis. Section III presents the survey of various differential cryptanalytic techniques that have been applied on the chaotic-based image encryption schemes. Section IV discusses the common weaknesses inherent in the encryption schemes and the possible improvements. Last section gives the concluding remarks.

2. Preliminaries: differential cryptanalysis

This section shows the general principles of the differential cryptanalysis that applies on the chaotic based image encryption scheme. Differential cryptanalysis can be considered as chosen plaintext attack, where the attacker is given access to choose pairs of inputs and outputs of a cipher. The concept of difference can be varied and interpreted in many ways. The most commonly used difference in the encryption scheme is either the exclusively-or operation ($\oplus$ or XOR) or the modular addition difference ($\boxplus$ or +). Let $X_1, X_2, \dots, X_n$ be the inputs of the encryption scheme with the corresponding outputs of $Y_1, Y_2, \dots, Y_n$ under the encryption with same secret key. Let ΔX_i be the input difference between two inputs and ΔY_i be the output difference between two outputs. We denote the difference between internal values as the intermediate difference between two input-output pairs when there exist many rounds in the cipher. Differential cryptanalysis utilizes the high probability of occurrences of a specific output difference (i.e. difference in the last round of the cipher) that is influenced by the input difference of the cipher. For illustration, an architecture of simple differential attack on an encryption scheme based on a S-box and XOR operations is shown in figure 1.

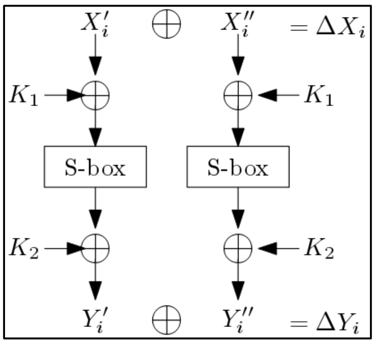

Figure 1. Illustration of an architecture of differential attack on an encryption scheme based on a S-box and XOR operations.

To perform differential attack, two inputs, X_i' and X_i'' are chosen to satisfy a particular ΔX_i, given that for the particular ΔX_i, ΔY_i will occur with high probability. For an ideal randomizing cipher, the probability of occurrence of ΔY_i given ΔX_i, $P(\Delta Y_i \mid \Delta X_i)$ is $\frac{1}{2^n}$, where n is the bit-length of X_i. With this property, the value of subkeys, $K_1$and K_2 can be guessed with lower time complexity than brute-force attack. A differential characteristic means a sequence of intermediate differentials that corresponds a particular input difference to a particular output difference. There exist multiple differential characteristics having same input and output differences but with different intermediate differences. Then, the combination of all of these differential characteristics with same input and output differences forms a differential. We can extend the application of differential cryptanalysis on block cipher to image encryption by dividing the images into block. The plain images will be the input of the cipher while the cipher images will be output of the cipher.

A differential for r consecutive rounds is normally known as r-round differential. According to Lu [32], the probability of a r-round differential can be defined as follows.

Definition 1. Suppose $\boldsymbol{E}$ is a m-bit block cipher and $K \in \{0,1\}^k$ is a key with size of k for $\boldsymbol{E}$. Let $P \in \{0,1\}^m$ be the plaintext block and $\boldsymbol{E}_K(P)$ be the corresponding ciphertext. Let a and b be two m-bit blocks and their differential (a, b) is written as $\Delta a \to \Delta b$. Then, the probability of $\Delta a \to \Delta b$ is defined as

$$Pr_{\boldsymbol{E}_k}(\Delta a \to \Delta b) = \underset{P \in \{0,1\}^m}{Pr}(E_K(P) \oplus E_K(P \oplus a) = b).$$

The next proposition follows trivially from Definition 1.

Proposition 2. If a and b are m-bit blocks, then

$$Pr_{\boldsymbol{E}}(\Delta a \to \Delta b) = \frac{|\{x|E(x) \oplus E(x \oplus a) = b, x \in \{0,1\}^m|}{2n}.$$

If the pair of plaintext and ciphertext are generated using random permutation, the possibility of occurrence of the output difference in the pair of images is 2^{-m}. If $\underset{\boldsymbol{E}}{Pr}(\Delta a \to \Delta b)$ is greater than 2^{-m}, then the cipher $\boldsymbol{E}$ can be distinguished with the sufficient number of chosen plaintext pairs.

3. Insight into various differential cryptanalytic techniques

Chaotic system has many inherent characteristics such as ergodicity, aperiodicity and highly sensitive to initial conditions and control parameters making it to be popular in designing an image encryption scheme [33]. The first chaotic based encryption algorithm was proposed by Matthews [34] and he showed that chaotic system can be applied to cryptography. A secure encryption algorithm must possess the confusion and diffusion functions in its algorithm [35]. Confusion can be attained by obscuring the relationship between cipher-image and the secret key. In other words, every pixel of cipher-image should be affected by secret key as many as possible. Besides, diffusion can reduce the redundancy of the plain-image by spreading it over the cipher-image. It also means that changing a pixel of plain-image will change a large number of pixels of cipher-image. In order to achieve good confusion and diffusion properties, the architecture of the chaotic based image encryption scheme can be designed based on permutation-only, diffusion-only, diffusion-permutation and permutation-diffusion. In this section, we discuss the research of the differential cryptanalysis based on these four categories.

3.1. Permutation-only algorithm

Permutation-only image encryption scheme encrypts the images by changing the positions of all the pixels of the image in a secret manner. The permutation process is an invertible function to allow a plain-image to be recovered from the decryption. Li *et al.* [36] proposed a general quantitative cryptanalysis on the multimedia algorithms against the known- or chosen-plaintexts attacks. The cryptanalysis was achieved by reconstructing the permutation matrix instead of recovering the key. They proved that only

$O(\log_L(MN))$ plain-images are needed to break the permutation-only algorithm, where MN is the size of the plain-image in terms of row and column and L is the number of possible different pixel values. The attack complexity of this cryptanalysis is $O(M^2N^2log_L(MN))$.

Li *et al.* [37] optimized the cryptanalysis in [36] by adopting a binary tree classification method and a multi-branch tree classification method. With these methods, the permutation-only algorithm can be broken with $O(\log_L(MN))$ plain-images, which is the same as [36]. However, the spatial and computational complexities are $O(MN)$ and $O(\lceil log_L(MN)\rceil \cdot MN)$, which are much lower than the attack complexity of the method in [36]. Therefore, the permutation-only algorithm has been proven to be insecure against plaintext attacks based on the cryptanalytic methods in [36,37]. The method has been applied by other researcher when performing differential attack [27].

3.2. Diffusion-only algorithm

Image encryption scheme that designed based on diffusion-only distribution is a poorer design as the confusion property has been neglected. Ye and Zhou proposed an image encryption schemes using diffusion-only algorithm [5]. They utilized hyper-chaotic system in the encryption schemes. Hyper-chaotic system can overcome the drawback of low dimensional chaos. Logistic map, tent map and Chebyshev map are the examples of one-dimensional chaotic maps that can be used to generate pseudorandom sequence. However, low dimensional chaos has small key space. Unlike low-dimensional chaotic systems, hyper-chaotic system has at least two positive Lyapunov exponents, larger key space, more complex dynamical characteristics and good sensitivity to initial conditions and control parameters.

Ye and Zhou [5] proposed a block image encryption that depends on double chaotic systems, i.e. Logistic map and 4D hyper-chaotic system. The authors claimed that the diffusion only architecture could overcome the problems inherent in permutation-diffusion process, such as many number of rounds required, permutation process can be easily exploited by known-plaintext attack and chosen-plaintext attack, and the key-dependent problem in the keystream. However, this architecture was attacked by Yap and Phan [24] using chosen-plaintext and chosen-ciphertext attacks with the exploitation on the r-round differential with probability of 1. This was also the first attack that demonstrates the vulnerability of image encryption scheme against distinguishing attack. Distinguishing attack is a cryptanalytic method that allows an attacker to distinguish the images encrypted by the underlying encryption algorithm from the random encrypted images [38]. A plaintext-ciphertext pairs with the input differential of $(0, \beta)$ were chosen. If the plaintext-ciphertext were generated by using proposed encryption scheme [5], then the output difference should also be $(0, \beta)$. The success rate of distinguishing the encrypted images from a truly random images is $1 - 2^{-8p}$, given that size of p pixels is 8-bit long. Besides, Yap and Phan also applied chosen-ciphertext attack on the Ye and Zhou's encryption scheme[24]. Chosen-ciphertext attack is a cryptanalysis where the attacker has the access to the decryption oracle to obtain the information of the plaintext without the knowledge of secret key [39]. Yap and Phan [24] pointed out that the encryption scheme [5] did not satisfy the confusion and diffusion properties due to the linear transformation function of images that uses the modular addition. The authors should investigate how the input difference can influence the output difference under the encryption. To improve the confusion and diffusion properties, addition-rotation-XOR (ARX) operations were suggested [24].

3.3. Diffusion-permutation algorithm

According to Wang *et al.* [40], diffusion-permutation algorithm is a poorer design as compared to permutation-diffusion due to low key sensitivity. There were two chaotic based image encryption schemes designed based on diffusion-permutation algorithm and were cryptanalyzed by using differential attack.

An image encryption based on a compound chaotic sequence was proposed by Tong and Chui [6]. The compound pseudo-random number sequence generated by two correlated chaotic maps was used to perform XOR substitution of the pixel values. Two chaotic maps were used to perform circular shift position permutations of rows and columns. However, Li *et al.* [25] pointed out that there are some defects found in the encryption scheme, making it vulnerable to the differential attack. The weaknesses include insensitivity of the scheme with respect to the changes of plaintexts, existence of weak and equivalent keys, and insufficient randomness of the compound chaotic sequence. Weak keys are referring to some fixed points of the chaotic maps that will affect the randomness of the chaotic sequences, while equivalent keys are referring to some different keys that will result in the same cipher-image, for any given plain-image [25]. Differential chosen-plaintext attack was implemented together with divide-and-conquer (DAC) attack. DAC attack is a method to break the encryption algorithms into two or more smaller components, until these components can be solved easily and directly. In[25], only three plain-images were required to solve for the row and column circular shift permutations, thereafter the XOR substitution was merely a simple XOR-based stream cipher which can be solved easily.

Dhall *et al.* [26] cryptanalyzed a four-round image encryption scheme involving hybrid 1D chaotic systems that made up by linearly combination of logistic map, tent map and sine map [7]. Multidimensional chaotic system can improve the security level of the cipher, but the downsides are resulting in the increase of difficulty level of hardware or software implementations and high computation complexity. To overcome this drawback, Zhou *et al.* [7] proposed a new chaotic system that could enhance the chaotic behavior of the chaotic map and also increase the chaotic ranges for the seed maps. Three hybrid chaotic systems suggested by them are Logistic-Tent system, Logistic-Sine system and Tent-Sine system. The four-round encryption scheme involves random pixel insertion, row separation, 1D substitution using Logistic-Tent system, row combination and image rotation. There are many weaknesses found in this encryption scheme by Dhall *et al.* [26]. They performed differential cryptanalysis on four-round encryption scheme without the knowledge of the key. They pointed out that the number of rounds of the encryption scheme was fixed and too small. The permutation step or rotation of the cipher images by $90°$ counter-clockwise was static and key-independent. There were $4M$ random pixels required to be inserted into M rows of image for each round. Even though the one-time usage of random pixels could provide certain level of security to the cipher, the huge amount of information to be communicated between the sender and receiver was practically infeasible in the real life application. The encryption scheme totally depended on the chaotic behaviour of the hybrid chaotic systems and omitted the importance of confusion and diffusion properties in the encryption. To improve this scheme, Dhall *et al.* [26] suggested to adopt key-based generation of random pixel instead of one-time used pixels. To enhance the confusion properties, key and plaintext-dependent permutation stage is suggested and to be performed before the substitution stage, so that the encryption will follow the permutation-substitution architecture. The fixed and small number of rounds can be solved by introducing a key-dependence of number of rounds with some lower and upper limit [26]. To improve the diffusion properties, instead of having the row-independent substitution process, inter-row feedback can be imposed in 1D-substitution. With these improvements, the desired confusion and diffusion properties of a secure encryption scheme can be satisfied.

3.4. Permutation-diffusion algorithm

Most of the chaotic based image encryption algorithms are based on permutation-diffusion algorithm. It is also known as Fridrich's algorithm because it was firstly proposed by Fridrich [41]. This is the most typical structure that fulfils confusion and diffusion and it had been widely used by other researchers in their ciphers. However, the permutation function of this kind of the encryption algorithm is independent of plaintext and the diffusion function, therefore it might expose to chosen plaintext attack and chosen ciphertext attack. The one-round encryption scheme based on this design is insecure and can be attacked by differential attacks [11,12,41,42]. Fridrich's algorithm with multi-round was attacked by Solak *et al.* [42] using the chosen ciphertext attack. However, the attack is getting harder with the increase of the number of rounds. Some minor defects of the attack proposed by Solak *et al.* was detected and the attack was further optimized by Xie *et al.* [43].

Behnia *et al.* [8] proposed a chaotic cryptographic scheme based on two composite polynomial chaotic maps. These two composition maps are used to perform the permutation and substitution processes of the encryption scheme. Li *et al.* [27] found that this encryption scheme was vulnerable to the differential attack. The attack involves three steps, breaking confusions I and II, and breaking permutation. The confusions I and II were solved by using the differential cipher-image and also the equivalent key. The remaining permutation process was solved by reconstructing the permutation matrix with $O(\log_L(MN))$ known or chosen plaintexts, where L is the number of different elements in the plaintexts. This method has been discussed by [36] in Subsection 3.1. Some other weaknesses found by the Li *et al.* [27] are insufficient randomness of pseudo-randomness number sequences and insensitivity of ciphertext to the change of plaintext.

Zhang *et al.* [9] proposed an image encryption scheme using alternate structure (IEAS) based on generalized cat map and one-way coupled map lattice (OCML) in 2007. In 2012, Zhang *et al.* [14] found that the proposed encryption scheme was vulnerable to differential attack. The equivalent secret key could be recovered when the integer parameter is even. Differential cryptanalysis was performed [14] in order to reveal the equivalent secret key of the encryption algorithm by studying the impact of differential plain-image on the differential cipher-image. Some other defects were found in the encryption scheme by Zhang *et al.* [14], i.e. small key space and insensitivity of ciphertext to the change of plaintext due to the implementation of linear operations, such as S-box in the encryption.

Yap *et al.* [28] applied impossible differential attack and DAC attack on the image alternate encryption algorithm based on chaotic map which was proposed by Wang and Guo [10]. Yap *et al.* [28] revisited the key space of Wang and Guo encryption scheme and found that the time complexity for a brute-force attack is $2^{150.053}$ which is smaller than $2^{159.453}$, the key space claimed by Wang and Guo. This shows that the encryption scheme is insecure. Impossible differential attack was applied on 9-round encryption scheme. This cryptanalysis was employing the miss-in-the-middle approach [44]. Since the number of round, $T = 9,$ then there was an 8-round impossible differential with the i-round and j-round differentials with probability of 1, for $i + j = 8$, where the intermediate differences of these two differential were an contradiction. In other words, the probability of i-round differential resulting in j-round differential is zero. Yap et al. [28] also applied a DAC attack on the encryption scheme by using a plain black image. These two methods demonstrated that the image encryption scheme proposed by Wang and Guo was insecure.

Fu *et al.* [11] proposed a medical image protection scheme based on chaotic systems in 2013. They claimed that bit-level permutation based on discrete cat map has a good confusion properties and able to attain the security level. However, Zhang *et al.* [45] later cryptanalyzed the one-round encryption of the proposed scheme. They demonstrate that the bit-level permutation does not practically add the additional strength to the cryptosystem. Zhang *et al.* also suggested permutation-substitution-permutation architecture could improve the current permutation-substitution structure. The suggestion was later criticized by Chen and Wang [29] because the permutation-substitution-permutation architecture is insufficient to resist differential attack. Instead of cryptanalyzing on one-round encryption, Chen and Wang [29] performed the differential cryptanalysis on multi-round original scheme and proved that the substitution keystream has no impact on the differential cipher-image and it depends only on the permutation step. They also proposed a new technique called double differential cryptanalysis comparison (DDCC) to attack three or more rounds of encryption.

Boriga *et al.* [12] proposed an image encryption scheme based on a two-dimensional hyper-chaotic map that derived from the equations of serpentine curve. The encryption algorithm follows a bi-modular architecture which consists of diffusion and confusion processes and depends on the two serpentine maps. The first serpentine map is adopted to generate random permutation vector and this vector is then used to shuffle the pixels of plain image. The second serpentine map is used to produce two keystreams and the keystreams will be used for the confusion process which alters the pixel values after permutation to reduce the correlation between the plain image and cipher image. A differential attack was performed on this encryption schemes by Wen *et al.* [30]. Wen *et al.* selected two special plain-images, P_1 and P_2, in which each pixel of the images was made up by the same value, but the pixel values for P_1 and P_2 are different. This is to eliminate the permutation effect in the algorithm and the encryption became diffusion only algorithm. The diffusion keystreams were revealed by XORing the two cipher-images and the image encryption scheme was broken.

Zhou *et al.* [13] proposed an image encryption algorithm based on skew tent map and Line map which adopted a permutation-substitution architecture. The skew tent map was used to generate three chaotic sequences which were used as the secret keys for the permutation and diffusion processes. The binary plain image was permutated using Line map. Chen *et al.* [31] applied differential cryptanalysis for one-round encryption with only $(M \times N - 1)$ chosen plain images. For two-round encryption, Chen *et al.* [31] applied forward differential and backward differential, or known as two-way differential comparison method in order to obtain permutation matrices for each round. Chen *et al.* [31] found that the differential cipher-image are independent of the diffusion keys which would substantially reduce the key space of the cryptosystem. The differential cipher-image also depends on a series of linear function of the differential plain-image. If one of the plain images was chosen to be a plain black image with all zero pixels, then the differential cipher-image solely depends on the other plain image and the permutation key. The cryptosystem was broken once the permutation key was revealed. However, permutation matrices for more than 2 rounds are difficult to be obtained by using these two methods. Since the differential cipher-image was formed by linear transformation of the differential plain-image, therefore Chen *et al.* used codebook attack to break the multi-round encryption algorithm. Codebook attack is a cryptanalytic method that the attacker attempts to construct a "codebook" which is a listing of ciphertexts that correspond to the plaintexts. Chen *et al.* [31] pointed out three important rules to have a secure permutation-diffusion encryption algorithm, i.e. having a self-synchronous key-stream, permutation process related to plain image, and a nonlinear and complicated diffusion rules.

3.5. Comparisons

All of the differential cryptanalyses discussed here have been summarized in table 1. Suppose that the plain image has the size of $M \times N$, where M is the number of row and N is the number of column. Let T be the number of round and r be the multi-round.

Table 1. Comparisons of Differential Cryptanalysis on Various Chaos Based Image Encryption Scheme

Reference		Chaotic Map used	Cryptanalysis Technique	Round	Image required	Time Complexity
Scheme	Attack					
Diffusion-only Algorithm						
[5]	[24]	Logistic Map Hyper-chaotic Map	Distinguishing Attack Chosen-ciphertext attack	r	2	$O(2 \cdot MN)$
Diffusion-Permutation Algorithm						
[6]	[25]	Compound chaotic sequence	Differential Attack Divide-and-Conquer Attack	1	3	$O(MN)$
[7]	[26]	Logistic-Tent Logistic-Sine Tent-Sine	Differential Attack	4	2	$O((MN)^3)$
Permutation-Diffusion Algorithm						
[8]	[27]	Composition Map	Differential Attack	1	$6 + \lceil log_L(MN) \rceil$	$O(M^2N^2\ log_L(MN))$
[9]	[14]	Generalized Cat Map One-way Coupled Map Lattice	Differential Attack	$T \leq 4$	5	$O(N^2 \cdot T!)$

[10]	[28]	Logistic Map	Impossible differential Attack Divide-and-Conquer Attack	$2 \leq T \leq 4$	$2^{\phi+16}$ 6	$2^{\phi+44.622}$. 9 encryptions $2^{119.023}$ encryptions
[11]	[29]	Cat map	Differential Attack Double differential cryptanalysis comparison	r	$16MN+1$	
[12]	[30]	Hyper-chaotic Map (Serpentine Map)	Differential Attack	1	2	$O(1 \cdot N)$
[13]	[31]	Skew Tent Map Line Map	Differential Attack Codebook Attack	r	$M \times N + 1$	$O(MN)$

4. Common defects inherent in the current encryption schemes

From the literature review, we found out that there are some common weaknesses in the chaotic based image encryption schemes and causing the encryption schemes vulnerable to the differential attack. The encryption operation involves the following weaknesses should be avoided in the design of a secure chaotic based image encryption scheme. The weaknesses and the suggested improvement are listed as follows.

4.1. Low sensitivity to the changes of plain-image

This is the major problem happening in the current image encryption scheme [5,6,8,9,13,14,24,25,27,31]. An ideal encryption algorithm should allow a bit of change in the plain-image leading to a large change in the cipher-image. However, linear transformation implemented in the encryption process, such as S-box and XOR operations violate the design rules of nonlinearity of the cryptography. To overcome this problem, nonlinear and complicated operations should be considered in the design of the algorithm [13,31].

A pixel of plaintext can only affect the higher pixel of the corresponding ciphertext and cannot influence other pixels of ciphertexts uniformly. The plaintext-dependent permutation should be implemented in encryption. To link the connection to other row of images, the substitution operation should apply inter-row feedback instead of performing substitution on rows independent of each other [7,26].

Besides, problem of independent of keystream from plain-image can be solved by applying the self-synchronous keystream [31].

4.2. Existence of weak and equivalent keys

Equivalent key causes same cipher-image to be generated using a particular plain-image under the encryption of some different keys [6,9,14,25]. This could reduce the key space and allow the attacker to access the information of the plain-image easily. Suppose the differential cipher-image is dependent on a series of functions and the differential plain image. If a special image, P_1 is chosen (e.g. all zero pixels) and with the information of equivalent key, another image P_2 can be recovered by inverting the function. On the other hand, weak key causes the encryption part fails at the certain fixed points of chaotic maps [6,25]. Therefore, it is important to identify the equivalent and weak keys of the chaotic systems.

4.3. Differential cipher-image is not related to keystream sequence

The keystream sequence was used as the permutation and diffusion keys in the encryption algorithms [11,13,29,31,45]. When there is irrelevance of differential cipher-image to the key-stream, then the key space would be greatly reduced. To overcome this problem, the key-dependent permutation and substitution processes should be implemented.

4.4. Insufficient randomness of pseudorandom number sequences

The chaotic system was not a good random number generator based on the random tests [6,8,25,27]. Random tests should be performed on chaotic systems to make sure the selected chaotic system can achieve the deterministic pseudo-randomness of the cryptography.

4.5. Number of rounds of the encryption scheme is fixed and small

The scheme could be decrypted easily if the encryption operations are simple, e.g. key-independent permutation and diffusion processes. To overcome this problem, Dhall *et al.* [26] suggested to implement an alternate forward and backward image encryption algorithms in the substitution stage. Key dependence number of rounds could also be implemented based on the availability of the resources and security requirements.

5. Conclusion

In this survey paper, the existing differential cryptanalysis on the chaotic based image encryption has been studied and analyzed. The current security evaluation method that relies on the conventional quantitative analysis is insufficient to demonstrate the strength of the encryption algorithms to resist this attack. The weaknesses of current chaotic based image encryption against differential cryptanalysis have been identified and discussed. During the construction of encryption algorithm, the author should avoid using the poorer designs mentioned in this paper. Besides, the author should know how the input difference of the encryption algorithm could affect its corresponding output difference. To make the chaotic based image encryption to be secure against differential attack, there are still many problems remained unsolved: (1) Study the weaknesses of the current statistical measures and provide an improved version of measures. (2) Explore other advanced cryptanalytic attacks that could threaten the security of the chaotic based image encryption. (3) Create a general rule to design a secure and efficient chaotic based image encryption scheme.

References

[1] Chai X, Chen Y and Broyde L 2017 A novel chaos-based image encryption algorithm using DNA sequence operations *Opt. Lasers Eng.* **88** 197–213

[2] Zhou N, Pan S, Cheng S and Zhou Z 2016 Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing *Opt. Laser Technol.* **82** 121–33

[3] Seyedzade S M, Mirzakuchaki S and Atani R E 2010 A novel image encryption algorithm based on hash function *Machine Vision and Image Processing (MVIP), 2010 6th Iranian* (IEEE) pp 1–6

[4] Zhang X, Zhao Z and Wang J 2014 Chaotic image encryption based on circular substitution box and key stream buffer *Signal Process. Image Commun.* **29** 902–13

[5] Ye G and Zhou J 2014 A block chaotic image encryption scheme based on self-adaptive modelling *Appl. Soft Comput.* **22** 351–7

[6] Tong X and Cui M 2008 Image encryption with compound chaotic sequence cipher shifting dynamically *Image Vis. Comput.* **26** 843–50

[7] Zhou Y, Bao L and Chen C L P 2014 A new 1D chaotic system for image encryption *Signal Processing* **97** 172–82

[8] Behnia S, Akhshani A, Mahmodi H and Akhavan A 2008 Chaotic cryptographic scheme based on composition maps *Int. J. Bifurc. chaos* **18** 251–61

[9] Zhang Y, Wang Y and Shen X 2007 A chaos-based image encryption algorithm using alternate structure *Sci. China Ser. F Inf. Sci.* **50** 334–41

[10] Wang X and Guo K 2014 A new image alternate encryption algorithm based on chaotic map *Nonlinear Dyn.* **76** 1943–50

[11] Fu C, Meng W, Zhan Y, Zhu Z, Lau F C M, Chi K T and Ma H-F 2013 An efficient and secure medical image protection scheme based on chaotic maps *Comput. Biol. Med.* **43** 1000–10

[12] Boriga R, Dăscălescu A C and Priescu I 2014 A new hyperchaotic map and its application in an

image encryption scheme *Signal Process. Image Commun.* **29** 887–901

[13] Zhou G, Zhang D, Liu Y, Yuan Y and Liu Q 2015 A novel image encryption algorithm based on chaos and Line map *Neurocomputing* **169** 150–7

[14] Zhang L Y, Li C, Wong K-W, Shu S and Chen G 2012 Cryptanalyzing a chaos-based image encryption algorithm using alternate structure *J. Syst. Softw.* **85** 2077–85

[15] Biham E and Shamir A 1991 Differential Crytanalysis of Des-Like Cryptosystems *J. Cryptol.* **4** 3–72

[16] Biham E and Shamir A 1991 Differential cryptanalysis of Feal and N-hash *Workshop on the Theory and Application of of Cryptographic Techniques* pp 1–16

[17] Biham E and Shamir A 1993 Differential cryptanalysis of the full 16-round DES *Differential Cryptanalysis of the Data Encryption Standard* (Springer) pp 79–88

[18] Biham E and Dunkelman O 2007 Differential Cryptanalysis in Stream Ciphers. *IACR Cryptol. ePrint Arch.* **2007** 218

[19] Knudsen L 1998 DEAL- a 128-bit block cipher *Complexity* **258** 216

[20] Biham E, Biryukov A and Shamir A 1999 Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials *International Conference on the Theory and Applications of Cryptographic Techniques* pp 12–23

[21] Wagner D 1999 The boomerang attack *International Workshop on Fast Software Encryption* pp 156–70

[22] Kelsey J, Kohno T and Schneier B 2000 Amplified boomerang attacks against reduced-round MARS and Serpent *International Workshop on Fast Software Encryption* pp 75–93

[23] Biham E, Dunkelman O and Keller N 2001 The rectangle attack—rectangling the Serpent *International Conference on the Theory and Applications of Cryptographic Techniques* pp 340–57

[24] Yap W-S and Phan R C-W 2017 Commentary on “A block chaotic image encryption scheme based on self-adaptive modelling”[Applied Soft Computing 22 (2014) 351--357] *Appl. Soft Comput.* **52** 501–4

[25] Li C, Li S, Chen G and Halang W A 2009 Cryptanalysis of an image encryption scheme based on a compound chaotic sequence *Image Vis. Comput.* **27** 1035–9

[26] Dhall S, Pal S K and Sharma K 2018 Cryptanalysis of image encryption scheme based on a new 1D chaotic system *Signal Processing* **146** 22–32

[27] Li C, Arroyo D and Lo K-T 2010 Breaking a chaotic cryptographic scheme based on composition maps *Int. J. Bifurc. Chaos* **20** 2561–8

[28] Yap W-S, Phan R C-W, Yau W-C and Heng S-H 2015 Cryptanalysis of a new image alternate encryption algorithm based on chaotic map *Nonlinear Dyn.* **80** 1483–91

[29] Chen L and Wang S 2015 Differential cryptanalysis of a medical image cryptosystem with multiple rounds *Comput. Biol. Med.* **65** 69–75

[30] Wen W, Zhang Y, Su M, Zhang R, Chen J and Li M 2017 Differential attack on a hyper-chaos-based image cryptosystem with a classic bi-modular architecture *Nonlinear Dyn.* **87** 383–90

[31] Chen L, Ma B, Zhao X and Wang S 2017 Differential cryptanalysis of a novel image encryption algorithm based on chaos and Line map *Nonlinear Dyn.* **87** 1797–807

[32] Lu J 2008 *Cryptanalysis of block ciphers* (University of London, UK)

[33] Kotulski, Zbigniew and Szczepański J 1997 Discrete chaotic cryptography *Ann. Phys.* **509** 381–94

[34] Matthews R 1989 On the derivation of a “chaotic” encryption algorithm *Cryptologia* **13** 29–42

[35] Shannon C E 1949 Communication theory of secrecy systems *Bell Labs Tech. J.* **28** 656–715

[36] Li S, Li C, Chen G, Bourbakis N G and Lo K T 2008 A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks *Signal Process. Image Commun.* **23** 212–23

[37] Li C and Lo K T 2011 Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks *Signal Processing* **91** 949–54

[38] Xiang T, Qu J and Xiao D 2014 Joint SPIHT compression and selective encryption *Appl. Soft Comput. J.* **21** 159–70

[39] Katz J and Yung M 2000 Unforgeable encryption and chosen ciphertext secure modes of operation *International Workshop on Fast Software Encryption* (Springer) pp 284–99

[40] Wang B, Xie Y, Zhou C, Zhou S and Zheng X 2016 Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps *Opt. J. Light Electron Opt.* **127** 3541–5

[41] Fridrich J 1998 Symmetric ciphers based on two-dimensional chaotic maps *Int. J. Bifurc. chaos* **8** 1259–84

[42] Solak E, Çokal C, Yıldız O T and Bıyıkoğlu T 2010 Cryptanalysis of Fridrich's chaotic image encryption *Int. J. Bifurc. Chaos* **20** 1405–13

[43] Xie E Y, Li C, Yu S and Lü J 2017 On the cryptanalysis of Fridrich's chaotic image encryption scheme *Signal Processing* **132** 150–4

[44] Biham E, Biryukov A and Shamir A 1999 Miss in the Middle Attacks on IDEA and Khufu *International Workshop on Fast Software Encryption* pp 124–38

[45] Zhang L, Zhu Z, Yang B, Liu W, Zhu H and Zou M 2015 Cryptanalysis and improvement of an efficient and secure medical image protection scheme *Math. Probl. Eng.* **2015**

Acknowledgments
The authors would like to thank Universiti Tunku Abdul Rahman (UTAR) for financially funding the research through the UTAR Research Fund number UTARRF 6200/W60.