IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 9, 2018, accepted November 19, 2018, date of publication November 27, 2018,
date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2883690

Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy

CHENGQING LI[1], DONGDONG LIN[1], BINGBING FENG[2], JINHU LÜ[3], AND FENG HAO[4]

[1]School of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[2]College of Information Engineering, Xiangtan University, Xiangtan 411105, China
[3]School of Automation Science and Electrical Engineering, Beihang University, Beijing 100083, China
[4]Department of Computer Science, University of Warwick, Coventry CV4 7AL, U.K.

Corresponding author: Chengqing Li (chengqingg@qq.com)

This work was supported by the Natural Science Foundation of China under Grant 61772447, Grant 61532020, and Grant U1736113.

ABSTRACT Recently, a chaotic image encryption algorithm based on information entropy (IEAIE) was proposed. This paper scrutinizes the security properties of the algorithm and evaluates the validity of the used quantifiable security metrics. When the round number is only one, the equivalent secret key of every basic operation of IEAIE can be recovered with a differential attack separately. Some common insecurity problems in the field of chaotic image encryption are found in IEAIE, e.g., the short orbits of the digital chaotic system and the invalid sensitivity mechanism built on information entropy of the plain image. Even worse, each security metric is questionable, which undermines the security credibility of IEAIE. Hence, IEAIE can only serve as a counterexample for illustrating common pitfalls in designing secure communication method for image data.

INDEX TERMS Chaotic cryptanalysis, multimedia cryptography, image encryption, secure communication, privacy protection.

I. INTRODUCTION

With the popularity of imaging sensors in smartphones and various video recording scenarios, e.g. dashboard camera and closed-circuit television (CCTV), a vast volume of multimedia data are recorded every day [1], [2]. Meanwhile, the fast network transmission technique allows them to be transmitted among cloud servers, social media platforms, and personal cellphones with ever-growing speed and scope. Once a multimedia file containing some personal privacy information leaves the original control scope, they may threaten the owner and the related persons very quickly. So, the security and privacy of multimedia data have become the concerns of everyone living in the cyberspace. To respond to such a challenge, a large number of multimedia privacy protections and preservation schemes were proposed in the past two decades [3], [4].

One of the well-known features of chaos is the so-called butterfly effect: if a butterfly flips its wings in Brazil, tomorrow Texas, USA will have a storm. In a more scientific term, we say a system is very sensitive to the initial condition, i.e., a small change at the very beginning will eventually lead to a completely different result. This implies unpredictability because an accurate measurement of the initial condition is in principle impossible. As the sensitivity and unpredictability are some good features we want to have in applications like secure communications and (pseudo-) random number generation, many researchers around the world have tried to apply chaos to build various cryptographic primitives: permutation relation [5], pseudo-random number generator [6], [7], hash function [8], private-key encryption scheme [9], [10], public-key encryption scheme [11], authentication [4], secure communication based on synchronization [12], secret-key share (agreement) algorithm [13], data hiding [14], and privacy protection [15]. The main objective of chaotic cryptanalysis is to disclose the information about the secret key of a chaotic encryption (or secure communication) scheme under all kinds of security models: *ciphertext-only attack* [5], *known-plaintext attack* [16], [17], *chosen-plaintext attack* [18], [19], *chosen-ciphertext attack* [20], and *impossible differential attack* [21]. Meanwhile, chaotic cryptanalysis also provides a novel perspective to study the dynamical properties of the underlying chaotic system. As degradation of any chaotic system definitely happens in a digital domain [22], [23], a chaos-based encryption scheme may own some special security defects that do not exist in the non-chaotic encryption schemes [24]–[26].

In [27], a chaotic image encryption algorithm was proposed using information entropy value calculated from the plain-image, which is named as IEAIE in this paper. In the algorithm, a pseudo-random number sequence generated by the two-dimensional Logistic-adjusted-Sine map (2D-LASM) proposed in [6] is used to control a combination of some basic operations, including position permutation and modulo addition. Especially, the information entropy of the plain-image is used to build up a sensitivity mechanism of the encryption result of IEAIE on the plain-image. This paper reports security defects of the chaos-based pseudo-random number generator and the sensitivity mechanism. As for one round version of IEAIE, its three basic parts can be broken with a strategy of the divide-and-conquer technique in the scenario of differential attack. In addition, each used security metric is questioned from the perspective of modern cryptanalysis.

The rest of the paper is organized as follows. Section II briefly introduces the algorithm IEAIE. Section III presents cryptanalysis of IEAIE by disproving security metrics used for IEAIE. The last section concludes the paper.

II. CONCISE DESCRIPTION OF IEAIE

IEAIE ignores any special storage format of image data and just treats it as text data, which is represented as a $M \times N$ 8-bit matrix $\mathbf{I}$.[1]

- *The secret key* is composed of two sets of initial conditions of 2D-LASM

$$\begin{cases} x_{i+1} = \sin(\pi \cdot \mu \cdot (y_i + 3) \cdot x_i \cdot (1 - x_i)), \\ y_{i+1} = \sin(\pi \cdot \mu \cdot (x_i + 3) \cdot y_i \cdot (1 - y_i)), \end{cases} \tag{1}$$

  (x_0, y_0) and (x'_0, y'_0), where $\mu \in [0.37, 0.38] \cup [0.4, 0.42] \cup [0.44, 0.93]$.
- *Keystream generation procedure*: 1) iterate 2D-LASM (1) from initial condition

$$\begin{cases} \bar{x}_0 = (x_0 + \dfrac{s+1}{s + x'_0 + y'_0 + 1}) \bmod 1 \\ \bar{y}_0 = (y_0 + \dfrac{s+2}{s + x'_0 + y'_0 + 2}) \bmod 1 \end{cases} \tag{2}$$

  $200 + \frac{M \cdot N}{2}$ times, and from the 201-th iteration, assign the obtained sequence into an $M \times N$ matrix $\mathbf{P}$ in the raster order, where

$$s = H(\mathbf{I}), \tag{3}$$

  $H(\mathbf{X})$ is the information entropy value of image block $\mathbf{X}$, namely

$$H(\mathbf{X}) = -\sum_{i=0}^{2^8-1} p(\phi_i) \cdot \log_2(p(\phi_i)), \tag{4}$$

  ϕ_i is the pixel of value i in $\mathbf{X}$, and $p(\phi_i)$ denotes the ratio between the number of ϕ_i in $\mathbf{X}$ and $M \cdot N$. In this paper, $x \bmod n = x - n\lfloor x/n \rfloor$, where $\lfloor \cdot \rfloor$ denotes the floor function.

  3) set

$$\begin{cases} \mathbf{u} = \lceil \mathbf{u}' \cdot 10^{14} \rceil \bmod M + 1, \\ \mathbf{v} = \lceil \mathbf{v}' \cdot 10^{14} \rceil \bmod N + 1, \end{cases} \tag{5}$$

  where $\mathbf{u}'$ is the a-th row of $\mathbf{P}$, $\mathbf{v}'$ is the b-th column of $\mathbf{P}$ (scalar multiplication and addition are performed if a matrix or vector is involved, the same hereinafter),

$$\begin{cases} a = \lceil (x_0 + y_0 + 1) \cdot 10^7 \rceil \bmod M + 1, \\ b = \lceil (x'_0 + y'_0 + 2) \cdot 10^7 \rceil \bmod N + 1, \end{cases} \tag{6}$$

  and $\lceil \cdot \rceil$ denotes the ceil function. Separately conduct the two vectors $\mathbf{u}$ and $\mathbf{v}$ with the following way: if there are elements of the same value, change one as the least number that does not exist in the updated vector.

  3) iterate 2D-LASM (1) from initial condition

$$\begin{cases} \bar{x}'_0 = (x'_0 + \dfrac{1}{x_0 + y_0 + 1}) \bmod 1 \\ \bar{y}'_0 = (y'_0 + \dfrac{2}{x_0 + y_0 + 2}) \bmod 1 \end{cases} \tag{7}$$

  $200 + \frac{M \cdot N}{2}$ times; starting from the 201-th iteration, transform every element of the generated sequence by

$$f(x) = \lceil x \cdot 10^{14} \rceil \bmod 256 \tag{8}$$

  and set the results into an $M \times N$ matrix $\mathbf{K}$ in the raster order.
- *Encryption procedure*:
  - *Horizontal permutation*: for $j = 1 \sim N$, move the j-th column of $\mathbf{I}$ to the $\mathbf{u}(j)$-th one of $\mathbf{B}^*$, namely $\mathbf{B}^*(:, \mathbf{u}(j)) = \mathbf{I}(:, j)$.
  - *Vertical permutation*: for $i = 1 \sim M$, move the i-th row of $\mathbf{B}^*$ to the $\mathbf{v}(i)$ row of $\mathbf{B}$, i.e. $\mathbf{B}(\mathbf{v}(i), :) = \mathbf{B}^*(i, :)$.
  - *Changing gray distribution with a constant matrix* $\mathbf{T}$: for $i = 1 \sim M, j = 1 \sim N$, do

$$\mathbf{R}(i, j) = (\mathbf{B}(i, j) + \mathbf{T}(i, j)) \bmod 256, \tag{9}$$

    where $\mathbf{T}(i, j) = M \cdot N + i + j$.
  - *Diffusion encryption:* for $i = 1 \sim M, j = 1 \sim N$, set

$$\begin{aligned} \mathbf{C}(i, j) = (&\mathbf{R}(i, j) + d_j \cdot \mathbf{C}(i, j-1) \\ &+ d_j \cdot \mathbf{K}(i, j) + \mathbf{K}(i, d_j)) \bmod 256, \end{aligned} \tag{10}$$

    where $\mathbf{C}(i, N+1) = \mathbf{C}(i, 0) \equiv 0$,

$$d_j = \lceil H(\mathbf{R}_j) \cdot 10^{14} \rceil \bmod N + 1, \tag{11}$$

    and $\mathbf{R}_j = \{\mathbf{R}(i, k)\}_{i=1, k=j+1}^{M, N}$.
- *Repeation:* Repeat the above four steps one more round.
- *Decryption procedure* is similar to the encryption one except the following points: 1) the order of the above four main steps is reversed; 2) every operation in each main step is replaced by its inverse version.

[1] The transform (5) in [27] cannot always generate bijective (one-to-one) permutation mapping and should be corrected to assure successful decryption of IEAIE.

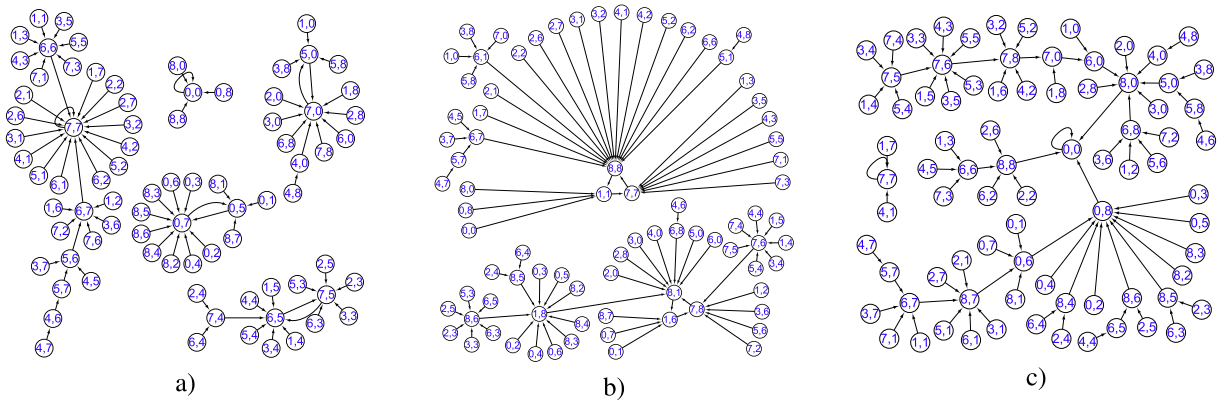


FIGURE 1. The functional graph of 2D-LASM under 3-bit fixed-point precision for different quantization strategies: a) floor; b) round; c) ceil, where the pair of numbers (i, j) in each node denotes coordinate $(i/2^3, j/2^3)$.

The horizontal and vertical permutations on the plain-image controlled by $\mathbf{u}$ and $\mathbf{v}$ can be equivalently represented by a permutation matrix $\mathbf{P}$ as [17], namely

$$\mathbf{B}(\mathbf{P}(i, j)) = \mathbf{I}(i, j), \tag{12}$$

where $i = 1 \sim M$, and $j = 1 \sim N$.

III. CRYPTANALYSIS

In [27], various aspects of IEAIE were analyzed to conclude that it owns superior security performance. However, we try to demonstrate that all the arguments are groundless.

A. SOME SECURITY DEFECTS OF IEAIE

In [18] and [24], some rules and suggestions for designing secure and efficient image encryption schemes were concluded. Some concrete steps for evaluating security performances of a chaotic image encryption schemes were given in [25]. Unfortunately, IEAIE did not follow the lessons summarized in [18], [24], and [25]. To attract the attention of designers of image encryption schemes on cryptanalysis, we check the security of every aspect of IEAIE and its test given in [27] as follows.

- **Underlying chaotic map**:
  In [6], a new two-dimensional chaotic map 2D-LASM was constructed by 'adjusting' Logistic map and Sine map with three strategies: cascading output of the former as the input of the latter; extending dimension of the phase plane from 1D to 2D; adopting one more multiplication variable with a constant delay parameter. It was proved that 2D-LASM can demonstrate much more complex chaotic behaviors than the two original 1D maps [28]. As shown in Fig. 1, any orbit will definitely enter a cycle after a transient process. Rigorous theoretical analyses given in [29] prove that the functional graph of any digital chaotic map is highly correlated with that in a domain with arithmetic precision as small as 3. As shown in Figs. 1, 2, the cycle length of the functional graph of 2D-LASM is very small for either arithmetic format. In [27], it was stated that "previously iterated values were discarded to avoid transient effects". Actually, the differences between neighboring states change exponentially along an orbit of any iterated map, which is different from the case for chaotic flow. The real purpose of discarding some initial iterated values is to avoid recovering the control parameters of the corresponding chaotic map from them, which is demonstrated in [16]. As shown in [29], some cycles of short period (even self-loop) always exist no matter which enhancement method is adopted, e.g. increasing the arithmetic precision, perturbing states, perturbing the control parameters, switching among multiple chaotic maps, and cascading among multiple chaotic maps. If the initial state is located in a small-scale connected component or a cycle of short period in the functional graph of the used chaotic map, there are not enough available states (200 states specified in [27, Sec. 3.1]) to be discarded. So, an adaptive threshold should be set to avoid this problem. But, it would cost additional computation.

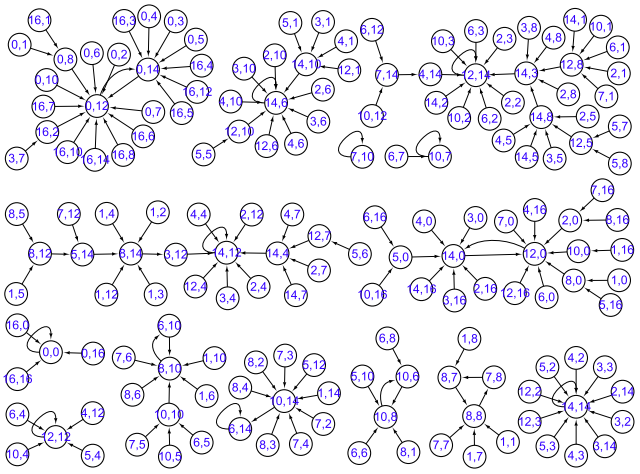


FIGURE 2. The functional graph of 2D-LASM with 6-bit floating-point precision and round quantization, where the length of mantissa fraction is 3.

a) b) c)

FIGURE 3. Two images with the same flat histogram: a) "Peppers"; b) "Lenna"; c) histogram of the images shown in Fig. 3a), b).

- **Key sensitivity**:
  In [27], "a small change of 10^{-14} is shifted in keys x_0, y_0, x_0', y_0'" to check their influence on the decryption results. Although 10^{-14} is small in itself as for our daily lives, the shift may cause a dramatic change of binary presentation of a number. Let's illustrate this problem with arithmetic format binary32 (single-precision floating-point format), where $10^{-14} = (1.01110100001001001011100)_2 \cdot 2^{-47}$ (stored as binary string "00101000001110100001001001011100"). As for number $10^{-12} = (1.00011001011110011001100)_2 \cdot 2^{-40}$ ("00101011100011001011110011001100"), $10^{-12} - 10^{-14} = (1.00010110101010010000010)_2 \cdot 2^{-40}$ ("00101011100010110101010010000010"). It can be calculated that 11 bits among the 23 fraction bits (underlined parts) of the subtracted number are changed. So, the four cases given in [27, Fig. 4] are far not enough to convince us anything. Now, we can see that a small decimal number should not be used to measure the change degree of initial condition in a binary computer. Observing Eq. (1), one can see that (x_0, y_0) and $(1 - x_0, 1 - y_0)$ are equivalent if 2D-LASM is implemented in a fixed-point arithmetic domain. Due to the modulo addition and division operation in Eq. (5), there may exist even much more equivalent secret keys. Besides these, quantization effects of the digital chaotic map may generate the same iteration orbit for different initial conditions (See Figs. 1, 2). So, the sensitivity of encryption results of IEAIE with respect to the change of its secret key is very weak.
- **Key space analysis**:
  In [27, Sec. 3.2.1], the precision of the secret key of IEAIE is fixed as 10^{-14}. In digital world, the precision can only be precisely specified by a power of two. If a floating-point number format (binary32 or binary64) is adopted, the distances between neighboring representable numbers are not uniform, which requires setting the length of mantissa fraction, and that of exponent, elaborately [29]. As shown in Fig. 1 and [28], there exists a number of nonchaotic regions of (x_0, y_0). The initial conditions falling in such regions may compose invalid or weak secret keys. So, we can conclude that the specification of IEAIE seriously violates Rule 5 suggested in [24], "The key space $\mathcal{K}$, from which valid keys are to be chosen, should be precisely specified and avoid nonchaotic regions." In addition, the computational complexity of checking each secret key and the valid time of the protected plain-image are not considered in [27]. In all, the statement "the brute-force attack is impossible to successfully execute" is unconvincing.
- **Histogram**:
  In [27], it was emphasized that "the histogram of the cipher-image should be or near uniform and be different from that of the plain-image after encryption". In fact, what counted for the security of IEAIE should be the matching degree between secret-key (or plain-image) and the histogram of the corresponding cipher-image. As shown in [19], an attacker can recover some statistical information of the plain-image by changing the counting objects of the histogram from pixel to bit. In addition, the spatial information of pixels may play a dominant role for the visual effect of the composed image. To show this point, Fig. 3 presents two 512×512 images with the same flat (exactly uniform) histogram, whose number of pixels for each tonal value is $\frac{512 \cdot 512}{256} = 1024$. Figure 4 gives the encryption results of the two images shown in Fig. 3 with the position permutation-only scheme HCIE cryptanalyzed in [17]. Although histograms of the two encrypted images kept unchanged, the scheme is secure enough for some application scenario, e.g. surveillance and protection of pay-TV from illegal users. Anyway, the three histograms calculated in terms of pixel shown in [27, Fig. 5] are not far enough to prove "the proposed algorithm has a good ability to frustrate the attack" based on the histogram.
- **Variance of histogram**:
  To further measure the uniformity degree of a cipher-image, the variance of its histogram was calculated

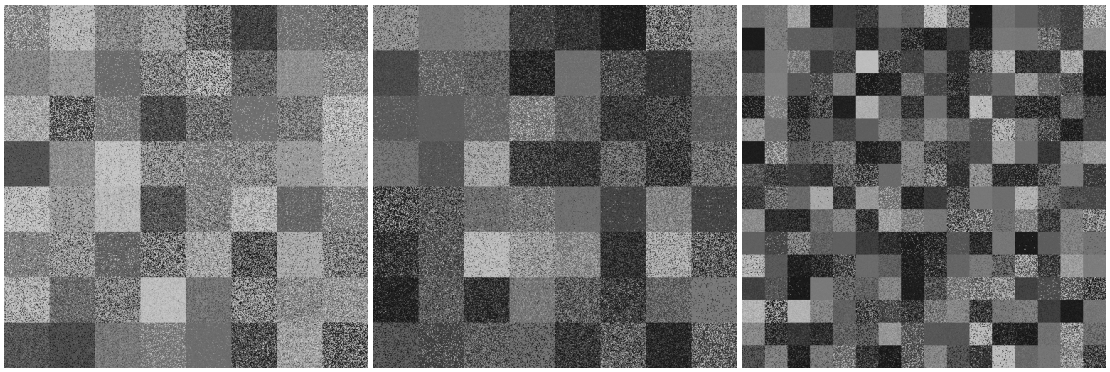


FIGURE 4. Three cipher-images encrypted by HCIE: a) "Peppers" with 64 × 64 blocks; b) "Lenna" with 64 × 64 blocks; c) "Lenna" with 32 × 32 blocks.

in [27]. Actually, the variance of a histogram cannot measure the number of different possible histograms generated by a tested encryption scheme. For example, the variances of two histograms "2, 2, 3, 4, 7" and "2, 2, 3, 5, 6" are different, but their number of different combinations are the same. But, the histogram variances of four cipher-images given in [27, Table 4] are far not sufficient to demonstrate existence of any rule. In addition, even some insecure encryption schemes can also make the obtained cipher-image own very low variance of histogram [30]. Moreover, visual security indexes of the three cipher-images shown in Fig. 4 are different, but the variances of the histogram of them are fixed to zero. In all, the statement "a lower variance represents higher uniformity" in [27] is not right.

- **Information entropy**:
  Information entropy is a quantitative metric measuring the disorder or randomness in a closed system. From Eq. (4), one can see that the entropy value of a message kept unchanged with respect to the following two kinds of changes: 1) permuting the position of every element within the message; 2) changing the elements of a given value as another one that does not exist in the message (if there is) [31]. In each case, the changes compose a bijection between specific domain and the corresponding codomain (See Fact 1). In all, there are a huge number of different images owning the same information entropy as a given image when its size is relatively large. For example, the five different images shown in Fig. 3, 4 share the same value of information entropy. Embedding Eq. (12) into Eq. (9), one can see that $H(\mathbf{R}_j)$ is determined by the two matrixes $\mathbf{P}$ and $\mathbf{T}$ for a given plain-image $\mathbf{I}$, where $j \in \{1, 2, \cdots, N\}$. From the definition of $\mathbf{R}_j$ and $\mathbf{T}$, one can deduce that every column of $\mathbf{T}$ should be of fixed value to assure that the modulo addition in Eq. (9) has the same effect on $\{\mathbf{R}_j\}_{j=1}^{N}$, namely every column of $\mathbf{R}$ (the difference between $\mathbf{R}_j$ and $\mathbf{R}_{j+1}$), for different plain-images. To satisfy such condition, $N \equiv 0 \pmod{256}$ should hold. Even this, the statement "the value of the information entropy is very sensitive to the message" given in [27, Sec. 2.1] is still baseless. Note that the tiny differences of entropy given in [27, Table 7] are only bounded by 0.01 and the cipher-image of "Lenna" encrypted by the analyzed bit-level permutation-only scheme cryptanalyzed in [5] can also reach as high as 7.978.
  Fact 1: For any function f, entropy function $H(\mathbf{X})$ (Eq. (4)) satisfies that $H(f(\mathbf{X})) \leq H(\mathbf{X})$ and the equality holds if and only if f is a bijection.
- **Plaintext sensitivity**:
  Plaintext sensitivity is very important for high-strength image encryption schemes as a plain-image and its slightly modified version (embedded by a watermark or some hiding messages) are often encrypted at the same time. If the used encryption scheme does not satisfy the sensitivity requirement, leakage of the cipher-image corresponding to one of the two similar plain-image may disclose the visual information of the other. In the field of image security, two metrics UACI (unified averaged changed intensity) and NPCR (number of pixels changing rate) are widely used to measure plaintext sensitivity. Unfortunately, the validity of the two metrics has been questioned in [30] by statistical information of the outputs of some insecure encryption schemes. Here, we emphasize that the internal structure of IEAIE cannot perform well to achieve the expected plaintext sensitivity. Observing the encryption procedure of IEAIE, one can see that all involved operations can make every operated bit 'run' from the least significant bit (LSB) to the most significant bit (MSB), not the opposite order. Concretely, the change of a bit in the i-th bit-plane (counted from the LSB to MSB) can only influence the bits in the $i \sim 8$-th ones. So, the influence scope of every bit of the plaintext on the corresponding ciphertext is dramatically different. No matter how many round numbers are repeated, this problem remains to exist [32]. The designers of IEAIE claimed that "the keystreams are different with respect to different plain-images" based on the assumption of high sensitivity of information entropy on change of the plain-image.

However, as we have explained above, this assumption is not correct. In all, the statement "a slight change in the plain-image leads to a completely different cipher-image" in [27, Sec. 3.2.2] is incorrect.

- **Coefficient correlation**:
  Just like most chaos-based image encryption schemes, [27] adopted the coefficient correlation of neighboring pixels of cipher-images encrypted by IEAIE to demonstrate its good security performance. As mentioned in [30, Fig. 3], there is "no clear (statistical) decision criterion for passing this test". Furthermore, three insecure encryption schemes deliberately constructed in [30] can perform very well in terms of fulfilling the metric. Actually, this metric can be calculated only from image encryption schemes working in the spatial domain. Reasonable security index of image data should consider the characteristics of the human visual system and the distribution of compressing coefficients of image data [33].
- **Efficiency analysis**:
  Ye *et al.* [27] claimed that IEAIE is suitable for real-time secure communication by comparing it with the image encryption scheme proposed in [6]. In fact, the fast running speed of IEAIE comes from less computation operations, namely the obtained efficiency is built on sacrificing security instead of better structure. In Eqs. (5), (6), (8), (11), IEAIE uses integer conversion functions following the general form

$$f_n(x) = f\left(10^m \cdot x\right) \bmod D, \tag{13}$$

  where m and D are positive integers, $f(x)$ is a quantization function, e.g. ceil and round. In processors, multiplication by a constant is implemented using a sequence of bit-wise shift and addition operations, e.g.

$$g(x) = ((x \lll 2) + x) \lll 1,$$

  where

$$x \lll s = \sum_{i=0}^{L-s-1} \left(x_i \cdot 2^{i+s}\right),$$

  $x = \sum_{i=0}^{L-1} x_i \cdot 2^i$, and L is the arithmetic precision. So the computational complexity of the conversion (13) is proportional to m [19]. In Eqs. (5), (6), (8), (11), m is set as 7 or 14. Only $\lceil \log_2 D \rceil$ bits are useful for IEAIE, the computation spent on generating the other $m\lceil \log_2(10) \rceil - \lceil \log_2 D \rceil$ bits are wasted. Taking Eq. (8) as an example, the utilization percentage of the computation cost on iterating 2D-LASM (1) is only $\frac{\lceil \log_2 D \rceil}{m\lceil \log_2(10) \rceil} = \frac{\lceil \log_2 256 \rceil}{14 \cdot \lceil \log_2(10) \rceil} = \frac{1}{7}$. In addition, the test on speed analysis in [27] was performed in the idea laboratory environment instead of resource-limiting real environments.

B. DIFFERENTIAL CRYPTANALYSIS

As shown in Fig. 5, an attacker can arbitrarily choose some plaintexts, $P_1, P_2, \cdots, P_{n-1}$, and the corresponding

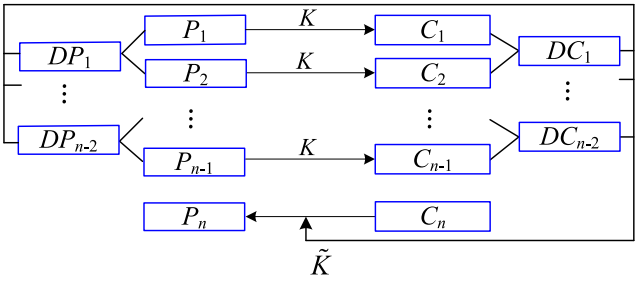


FIGURE 5. The model of differential attack.

ciphertexts, $C_1, C_2, \cdots, C_{n-1}$, encrypted by the same secret key K in the scenario of chosen-plaintext attack. As for differences between plaintexts P_i and P_{i+1}, $DP_1, DP_2, \cdots, DP_{n-1}$, one can observe the corresponding differences between ciphertexts C_i and $C_{i+1}, DC_1, DC_2, \cdots, DC_{n-1}$. The differences are defined in terms of an invertible operation used in the encryption scheme, e.g. bitwise OR and modulo subtraction. So differential cryptanalysis can be considered as a chosen-plaintext attack on a weakened version of the analyzed encryption scheme for some differences selected from $\binom{n}{2} = n(n-1)/2$ possible ones. In the broadest sense, *differential cryptanalysis* is a cryptanalytic method studying how particular differences in plaintext pairs affect the resultant differences, which is also called *differential*, of the corresponding ciphertext pairs. Considering the public structure of the analyzed encryption scheme, some basic parts can be deliberately canceled and the remaining part can be broken with much less resources. By repeating the process, the equivalent secret key of the whole encryption scheme $\tilde{K}$ can be recovered, which is then used to decrypt another ciphertext C_n, encrypted by the same secret key.

From the above introduction of the chosen-plaintext attack, one can see that the attack model relies on repeating usage of the secret key. So the designers of IEAIE use the information entropy of the plain-image to "affect the usage of the keystream and frustrate the chosen-plaintext and known-plaintext attacks" in [27, Sec. 2.2]. However, based on the analysis on the insensitivity of information entropy in above sub-section, it is very easy to construct some plain-images possessing the same keystream during the encryption process of IEAIE. Observing the encryption procedure of IEAIE, one can see that its real operations are solely determined by $N + 1$ parameters, s and $\{d_j\}_{j=1}^{N}$. Note that even when two plain-images generate different entropy values in the encryption process, their corresponding key steams are still maybe the same due to the following reasons: 1) the modulo addition and division in Eq. (2) may make different sets of $(x_0, y_0, x_0', y_0', s)$ result in the same value of $(\bar{x}_0, \bar{y}_0)$; 2) the quantization error of calculating $\log_2(\cdot)$ in computer may make different combinations of $\{\phi_i\}_{i=0}^{2^8-1}$ generate the same value of $H(X)$; 3) Eq. (11) only extract $\lceil \log_2(N) \rceil$ bits of intermediate computing result of $\mathbf{R}_j$, and may output the same value of d_j for different inputs of $\mathbf{R}_j$. Once the dependability

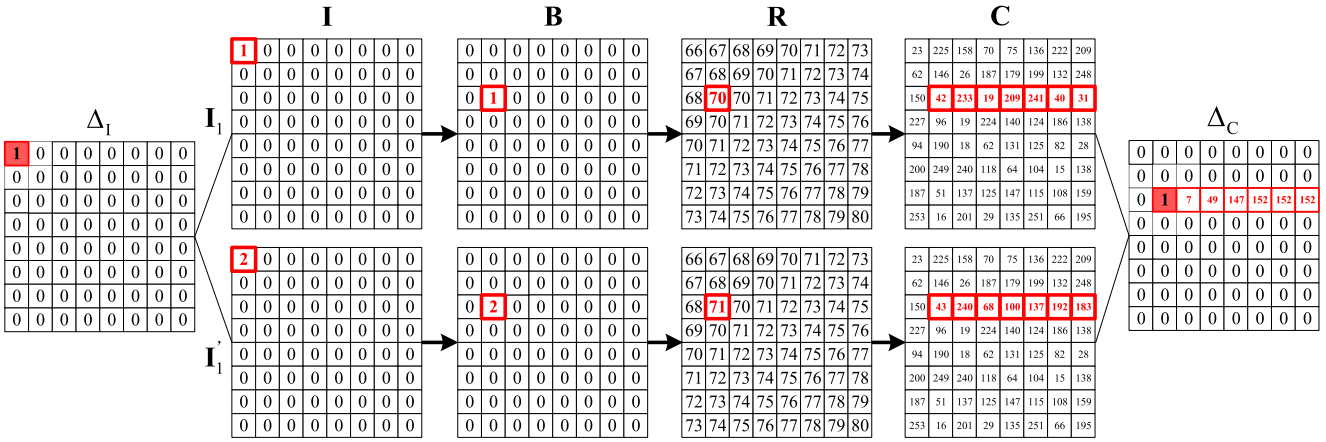


FIGURE 6. The process of revealing the permutation procedure of IEAIE with a differential attack.

mechanism of the key stream of IEAIE on the plain-image is concealed, the structure of Eq. (10) becomes the same as that of the main function of the image encryption scheme cryptanalyzed in [19]. Then, the differential cryptanalysis on IEAIE can be performed similarly.

Assume two plain-images $\mathbf{I}$ and $\mathbf{I}'$ own the same set of s and $\{d_j\}_{j=1}^{N}$ in the encryption process of IEAIE. As for their difference in terms of modulo subtraction $\Delta\mathbf{I}$, IEAIE is degenerated to

$$\begin{cases} \Delta\mathbf{R}(\mathbf{P}(i,j)) = \Delta\mathbf{I}(i,j), \\ \Delta\mathbf{C}(i,j) = (\Delta\mathbf{R}(i,j) + d_j \cdot \Delta\mathbf{C}(i,j-1)) \bmod 256, \end{cases} \tag{14}$$

where $i = 1 \sim M$, $j = 1 \sim N$, $\Delta\mathbf{C}$ is the difference of the corresponding cipher-images of $\mathbf{I}$ and $\mathbf{I}'$ in terms of the operator (some components in Eq. (10) are eliminated by the modulo subtraction), and $\Delta\mathbf{C}(i,0) \equiv 0$. Observing Eq. (14), one can assure that

$$\mathbf{P}(i^*, j^*) = (i^{**}, j^{**}) \tag{15}$$

if $\Delta\mathbf{I}$ has only one non-zero element at entry (i^*, j^*), where (i^{**}, j^{**}) is the entry of the first non-zero element in differential Δ_C (counted in the scan order).

Based on the above analysis, the differential cryptanalysis on one round version of IEAIE can be described as follows.

- *Step 1*: Choose two plain-images of size $M \times N$, $\mathbf{I}$ and $\mathbf{I}'$, satisfying

$$\begin{cases} \mathbf{I}(i^*, j^*) = a, \\ \mathbf{I}'(i^*, j^*) = b, \\ \mathbf{I}(i,j) = c, \\ \mathbf{I}'(i,j) = c, \end{cases}$$

  where a, b, c are non-negative integers and $\#\{a,b,c\} = 3$, $(i,j) \in \{(1,1),(1,2),\cdots(M,N)\} \setminus (i^*, j^*)$, and $\#\{\cdot\}$ denotes the cardinality of a set. Note that (i^*, j^*) is initialized as $(1, 1)$.

- *Step 2*: Let $\mathbf{I}$ and $\mathbf{I}'$ pass through the encryption process of IEAIE with an unknown secret key and obtain the corresponding cipher-images, $\mathbf{C}$ and $\mathbf{C}'$.
- *Step 3*: Get the value of $\mathbf{P}(i^*, j^*)$ via Eq. (15).
- *Step 4*: Repeat the above procedure for $(i^*, j^*) = (1,2), (1,3) \sim (M, N-1)$ (selected in the scan order of a matrix of size $M \times N$) and get the value of $\mathbf{P}(i^*, j^*)$. The value of $\mathbf{P}(M, N)$ can be identified as the sole unused location.
- *Step 5*: Recover $\mathbf{R}$ by Eq. (12) and calculate

$$\mathbf{D}(i,j) = (\mathbf{C}(i,j) - \mathbf{R}(i,j) - d \cdot \mathbf{C}(i,j-1)) \bmod 256$$

  for $i = 1 \sim M$ and $j = 1 \sim N$.

Observing Eq. (10), one can see that $\mathbf{D} = \{\mathbf{D}(i,j)\}_{i=1,j=1}^{M,N}$ can work as the equivalent version of the secret key for decryption on the *diffusion encryption* part. In all, two matrixes $\mathbf{P}$ and $\mathbf{D}$ can work as the equivalent secret key of IEAIE.

A number of experiment were performed to verify performance of the above attacking steps. A concrete case of revealing the permutation relationship of IEAIE on a plain-image of size 8×8 is shown in Fig. 6, where $x_0 = 0.0056$, $y_0 = 0.3678$, $x_0' = 0.6229$, and $y_0' = 0.7676$, and $\mu = 0.8116$. In this case, the same set of s and $\{d_j\}_{j=1}^{8}$ are generated for the two toy plain-images due to the quantization effect. From Fig. 6, we can see that the new permuted location of the sole non-zero element at entry $(1, 1)$ in the differential plain-image can be observed by searching for the first different elements of the two cipher-images.

In [27], two rounds of the basic operations are suggested. Here, we skip the cryptanalysis of the full version of IEAIE based on the following considerations: 1) existence of the security defects presented in the above sub-section is not related with the round number; 2) cryptanalysis of the two rounds of IEAIE involves very complex deduction and presentation; 3) the reported security defects of IEAIE are far enough to demonstrate that it cannot be fixed by simple modifications.

IV. CONCLUSION

This paper analyzed the security of a chaotic image encryption algorithm based on information entropy, IEAIE. The claimed superiorities of its structure are analyzed in detail and are found incorrect. Furthermore, every used security metric is incapable to testify real security performance. To design a secure and efficient multimedia encryption scheme, the related critical factors, e.g. the special properties of multimedia data, the concrete application scenario with specified constraints, computation load, should be considered comprehensively. Much cryptanalytic works need to be done to bridge the gap between the field of nonlinear dynamics and that of modern cryptography.

REFERENCES

[1] H. Li, K. Wang, X. Liu, Y. Sun, and S. Guo, "A selective privacy-preserving approach for multimedia data," *IEEE Multimedia*, vol. 24, no. 4, pp. 14–25, Oct./Dec. 2017.

[2] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.

[3] X. Zhang, S.-H. Seo, and C. Wang, "A lightweight encryption method for privacy protection in surveillance videos," *IEEE Access*, vol. 6, pp. 18074–18087, 2018.

[4] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 824–839, Sep. 2018.

[5] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE Multimedia*, vol. 24, no. 3, pp. 64–71, 2017.

[6] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[7] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

[8] Z. Lin, S. Yu, and J. Lü, "A novel approach for constructing one-way hash function based on a message block controlled 8D hyperchaotic map," *Int. J. Bifurcation Chaos*, vol. 27, no. 7, p. 1750106, 2017.

[9] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, 2012.

[10] Q. Shen and W. Liu, "A novel digital image encryption algorithm based on orbit variation of phase diagram," *Int. J. Bifurcation Chaos*, vol. 27, no. 13, Dec. 2017, Art. no. 1750204.

[11] A. Shakiba, M. R. Hooshmandasl, and M. A. Meybodi, "Cryptanalysis of multiplicative coupled cryptosystems based on the chebyshev polynomials," *Int. J. Bifurcation Chaos*, vol. 26, no. 7, p. 1650112, 2016.

[12] M. H. Abd, F. R. Tahir, G. A. Al-Suhail, and V.-T. Pham, "An adaptive observer synchronization using chaotic time-delay system for secure communication," *Nonlinear Dyn.*, vol. 90, no. 4, pp. 2583–2598, 2017.

[13] L. Zhang, S. Zhu, and S. Tang, "Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 2, pp. 465–475, Mar. 2017.

[14] X. Ge, B. Lu, F. Liu, and D. Gong, "An image encryption algorithm based on information hiding," *Int. J. Bifurcation Chaos*, vol. 26, no. 11, Oct. 2016, Art. no. 1650192.

[15] J. Sun, X. Liao, X. Chen, and S. Guo, "Privacy-aware image encryption based on logistic map and data hiding," *Int. J. Bifurcation Chaos*, vol. 27, no. 5, May 2017, Art. no. 1750073.

[16] C. Li, T. Xie, Q. Liu, and G. Chen, "Cryptanalyzing image encryption using chaotic logistic map," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 1545–1551, 2014.

[17] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Process.*, vol. 118, pp. 203–210, Jan. 2016.

[18] S. Li, C. Li, G. Chen, and K.-T. Lo, "Cryptanalysis of the RCES/RSES image encryption scheme," *J. Syst. Softw.*, vol. 81, no. 7, pp. 1130–1143, 2008.

[19] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia*, to be published.

[20] X. Ge, B. Lu, F. Liu, and X. Luo, "Cryptanalyzing an image encryption algorithm with compound chaotic stream cipher based on perturbation," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 1141–1150, 2017.

[21] W.-S. Yap, R. C.-W. Phan, W.-C. Yau, and S.-H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dyn.*, vol. 80, no. 3, pp. 1483–1491, 2015.

[22] Q. Wang *et al.*, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 3, pp. 401–412, Mar. 2016.

[23] Y. Liu, Y. Luo, S. Song, L. Cao, and J. Liu, "Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation," *Int. J. Bifurcation Chaos*, vol. 27, no. 3, 2017, Art. no. 1750033.

[24] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[25] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, 2018.

[26] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[27] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *Int. J. Bifurcation Chaos*, vol. 28, no. 1, 2018, Art. no. 1850010.

[28] Z. Hua, B. Zhou, and Y. Zhou, "Sine-transform-based chaotic system with FPGA implementation," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2557–2566, Mar. 2018.

[29] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen. (2017). "Dynamic analysis of chaotic maps as complex networks in the digital domain." [Online]. Available: https://arxiv.org/abs/1410.7694

[30] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[31] M. Madiman, A. W. Marcus, and P. Tetali, "Entropy and set cardinality inequalities for partition-determined functions," *Random Struct. Algorithms*, vol. 40, no. 4, pp. 399–424, 2012.

[32] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.*, vol. 132, pp. 150–154, Mar. 2017.

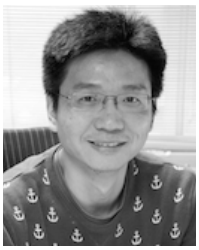
[33] T. Xiang, S. Guo, and X. Li, "Perceptual visual security index based on edge and texture similarities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 951–963, May 2016.

CHENGQING LI received the M.Sc. degree in applied mathematics from Zhejiang University, China, in 2005, and the Ph.D. degree in electronic engineering from the City University of Hong Kong in 2008. From 2008 to 2010, he was a Post-Doctoral Fellow with The Hong Kong Polytechnic University. In 2010, he was with the College of Information Engineering, Xiangtan University, China. From 2013 to 2014, he was with the University of Konstanz, Germany, under the support of the Alexander von Humboldt Foundation. He is currently a Full Professor with the School of Computer Science and Electronic Engineering, Hunan University. He focuses on security analysis of multimedia encryption schemes and privacy protection schemes. He has published about 50 papers on the subject in the past 13 years, receiving more than 2500 citations with an h-index of 28. He is serving as an Associate Editor for the *International Journal of Bifurcation and Chaos*.

DONGDONG LIN received the B.Sc. and M.Sc. degrees in computer science from the College of Information Engineering, Xiangtan University, China, in 2015 and 2018, respectively. He is currently visiting at the School of Computer Science and Electronic Engineering, Hunan University, China. His research interests include cryptanalysis and image privacy protection.

BINGBING FENG received the B.Sc. and M.Sc. degrees in computer science from the College of Information Engineering, Xiangtan University, in 2015 and 2018, respectively. His research interests include complex networks and nonlinear dynamics.

JINHU LÜ received the Ph.D. degree in applied mathematics from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, in 2002. He was a Professor with RMIT University, Australia, and a Visiting Fellow with Princeton University, USA. He is currently a Professor with the Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He has authored three research monographs and more than 110 SCI journal papers published in the fields of complex networks and complex systems, nonlinear circuits and systems, receiving more than 8000 SCI citations with an h-index of 42. He is an ISI Highly Cited Researcher in Engineering.



FENG HAO received the Ph.D. degree in computer security from the Computer Laboratory, University of Cambridge, in 2007. He worked in security industry for several years before joining Newcastle University as a Lecturer in 2010. He was promoted to the readership in 2014. He is currently a Professor of security engineering with the Department of Computer Science, University of Warwick. His research interests include applied cryptography, security engineering, and efficient computing.