On the Security of Permutation-Only Image Encryption Schemes

Alireza Jolfaei, Xin-Wen Wu, *Senior Member, IEEE*, and Vallipuram Muthukkumarasamy

***Abstract*— Permutation is a commonly used primitive in multimedia (image/video) encryption schemes, and many permutation-only algorithms have been proposed in recent years for the protection of multimedia data. In permutation-only image ciphers, the entries of the image matrix are scrambled using a permutation mapping matrix which is built by a pseudo-random number generator. The literature on the cryptanalysis of image ciphers indicates that the permutation-only image ciphers are insecure against ciphertext-only attacks and/or known/chosen-plaintext attacks. However, the previous studies have not been able to ensure the correct retrieval of the complete plaintext elements. In this paper, we revisited the previous works on cryptanalysis of permutation-only image encryption schemes and made the cryptanalysis work on chosen-plaintext attacks complete and more efficient. We proved that in all permutation-only image ciphers, regardless of the cipher structure, the correct permutation mapping is recovered completely by a chosen-plaintext attack. To the best of our knowledge, for the first time, this paper gives a chosen-plaintext attack that completely determines the correct plaintext elements using a deterministic method. When the plain-images are of size $M \times N$ and with L different color intensities, the number n of required chosen plain-images to break the permutation-only image encryption algorithm is $n = \lceil \log_L(MN) \rceil$. The complexity of the proposed attack is $O(n \cdot MN)$ which indicates its feasibility in a polynomial amount of computation time. To validate the performance of the proposed chosen-plaintext attack, numerous experiments were performed on two recently proposed permutation-only image/video ciphers. Both theoretical and experimental results showed that the proposed attack outperforms the state-of-the-art cryptanalytic methods.**

***Index Terms*— Chosen-plaintext attack, cryptanalysis, image encryption, permutation.**

I. Introduction

THE FAST growing demand for digital multimedia applications has opened up a number of challenges regarding the confidentiality of images and videos in many multimedia-based services, such as Pay-TV, remote video conferencing, and medical imaging. Reliable storage and secure transmission of visual content is a legitimate concern of Intellectual Property (IP) owners. Thus, there is a strong need to protect images and videos against unauthorized use or other security violations. Encryption is a solution to maintain confidentiality. Multimedia encryption obfuscates the image/video datastream to ensure secure transmission of image/video data between two parties over a public channel. Given the fact that raw video data is constructed by a sequence of still images (frames), image encryption techniques can be applied to still images or single frames in a video.

Since the 1970s, a large number of encryption schemes have been proposed, some of which have been standardized and widely adopted all over the world, such as Data Encryption Standard (DES) [1] and Advanced Encryption Standard (AES) [2]. However, the problem of image encryption is beyond the application of established and well-known encryption algorithms. This is primarily due to the constraints imposed by the data structure and the application requirements, such as format compliance [3], real-time performance [4], complexity [5], compression efficiency [6], perceptibility [7] and the security level [8]. To address these concerns, significant attempts have been made to develop robust encryption schemes for the image data [9]–[11].

Due to the grid structure of digital images, image encryption methods utilize three different types of operations: position permutation, value transformation, and the combination form. Among different operations, permutation (transposition) is a commonly used primitive in many image encryption schemes. This is mainly due to the easy implementation and applicability of permutation in both spatial and frequency domains. In addition, by combining permutation with other simple value transformation operations, such as XOR, a highly secure multimedia encryption scheme can be achieved. In all the well-known permutation-only ciphers, image entries (or bit-planes) are permuted by a mapping matrix which is built by a pseudo-random number generator. From the design point of view, permutation dissipates the statistical structure of the plaintext into long range statistics and it is suitable for fast processing requirements of massive digital multimedia data [12], [13].

Despite the advantages of permutation, it has a number of inherent limitations. Permutation-only ciphers disclose some essential characteristics of the plaintext, such as the frequency distribution of symbols in the plaintext. Also, when the size of plaintext is small, that is, the number of possible arrangements for the plaintext elements is less than the key space, the number of effective keys can be reduced, and hence, the permutation mapping can be disclosed. Moreover, permutation-only encryption/decryption are not simple sequential operations that can be done dynamically.

Manuscript received April 11, 2015; revised July 24, 2015 and September 16, 2015; accepted September 30, 2015. Date of publication October 9, 2015; date of current version December 9, 2015. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Hitoshi Kiya.

The authors are with the School of Information and Communication Technology, Griffith University, Gold Coast, QLD 4222, Australia (e-mail: alireza.jolfaei@griffithuni.edu.au; x.wu@griffith.edu.au; v.muthu@griffith.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2489178

In general, permutation may need a buffer with a size comparable to that of the plaintext. Therefore, due to the limitations above, permutation-only ciphers are nowadays only used in applications where substitution is technically infeasible and/or only a moderate level of protection is required. Considering typical examples of permutation-only image ciphers, in [14]–[16] image entries are dislocated using pseudo-random permutations; in [17] and [18] permutation operations are performed on the bit-planes of the image entries; and in [19] and [20] permutation operations are performed on DCT/wavelet coefficients.

The security of permutation-only image encryption schemes has been studied for a long time, and it has been shown that most of such schemes are insecure against ciphertext-only attacks and/or known/chosen-plaintext attacks, which is due to the high information redundancy in the multimedia data and some specific weaknesses in the encryption algorithms [21]–[23]. Despite the extensive cryptanalysis of permutation-only multimedia ciphers, in recent years, many permutation-only ciphers have been proposed for the protection of multimedia data, including digital images [15], [17], [18] and video [16], [19], [20]. This is mainly because the above-mentioned cryptanalytic methods can only be applied to specific encryption methods and cannot be generalized to a wider class of permutation-only multimedia ciphers [24]–[27]. In addition, even the best known methods of known/chosen-plaintext attacks ([28], [29]) cannot ensure the complete retrieval of the correct plaintext content, and hence, it is still ambiguous as to whether the security of permutation-only image ciphers can be effectively improved by designing new methods to generate better pseudo-random permutations.

This paper presents a cryptanalysis which breaks most (if not all) permutation-only multimedia ciphers. In fact, it is shown that all permutation-only image ciphers are completely broken by chosen-plaintext attacks and no better pseudo-random permutation mapping can be realized to offer a higher level of security against chosen-plaintext attacks. For a successful attack, we derived a tight lower bound for the required number n of chosen plain-images, that is, $n = \lceil \log_L (MN) \rceil$, comparing to the currently known results $O\left(\lceil \log_L (MN) \rceil\right)$ [28], [29], where MN is the size of the image and $L-1$ is the maximum color intensity, that is, a color intensity is specified by $l\,(0 \leq l \leq L-1)$. The computational complexity of the proposed attack is $O\,(n \cdot MN)$. To verify the feasibility of the proposed attack, experiments were performed on the recently proposed permutation-only image ciphers by Rahman et al. [16] and Fu et al. [17]. Our experimental results support the theoretical results that pseudo-random permutations alone cannot provide sufficient security against chosen-plaintext attacks. Compared to the state of the art cryptanalytic methods of [28] and [29], which partially (quantitatively) determine the permutation mapping, our chosen-plaintext attack gives a precise procedure for the careful construction of the required chosen plain-images, and therefore, completely discloses the correct permutation mapping with less data and computational complexity.

The rest of this paper is organized as follows. Section 2 reviews the related work in the cryptanalysis of permutation-only image ciphers. In section 3, the procedure of the chosen-plaintext attack is described. Section 4 overviews two typical permutation-only image ciphers (case studies) proposed by Rahman et al. [16] and Fu et al. [17]. Experimental results are shown in Section 5 to support the theoretical cryptanalysis. Section 6 discusses the advantages of the proposed chosen-plaintext attack in comparison to the state of the art cryptanalyses. Finally, the last section concludes the paper.

II. Related Work

The security of permutation-only image ciphers has been extensively studied. These cryptanalytic studies are briefly described as follows. In [24], Matias and Shamir analyzed the security of early permutation-only image encryption schemes used in analog broadcasting systems. The prominent feature of such ciphers were that they utilized fewer numbers of permutations with shorter domains, with the intention of keeping the bandwidth increase of the encryption process as low as possible. This made the early permutation-only image encryption schemes more vulnerable to correlation attacks, implying that the high correlation properties remaining in the permuted images could be employed to restore the image. To address the correlation issues, Matias and Shamir proposed a permutation-only scheme which scanned pixels in a highly irregular scanning pattern using a pseudo-random space filling curve. Bertilsson et al. [25] then showed that Matias and Shamir's permutation method is vulnerable to a ciphertext-only attack. They showed that the pixel data could be reordered according to a space-filling curve, and hence, the plain-image could be partially recovered by exploiting the correlation between subsequent frames.

Later, Kuhn [26] presented a more advanced approach to break the video signal scramblers commercially employed within pay-TV conditional access encryption systems [30], such as EuroCrypt, VideoCrypt and Nagravision, using ciphertext-only attacks. Kuhn showed that the long portion of the permuted lines/segments makes the correlation attacks on the scrambling algorithm feasible by comparing and matching lines/segment portions. Li et al. [27] then extended Kuhn's work by analyzing the permutation domain of particular image encryption schemes with longer permutation domains, such as the row-column permutation-only encryption scheme of [14]. Despite the efforts made to improve the performance of previous ciphertext-only attacks, these attacks are only applicable to schemes whose permutation domains are considerably smaller than the size of input images. Indeed, increasing the permutation domain makes the correlation analysis, and hence the ciphertext-only attacks, computationally cumbersome.

To reduce the complexity of the exhaustive key search (a ciphertext-only attack), Li et al. [28] provided a general cryptanalysis (a known-plaintext attack and a chosen-plaintext attack) based on the quantitative relation between the breaking performance and the number of required known/chosen plaintexts. They showed that the number n of required known/chosen plain-images to perform a successful known/chosen-plaintext attack on a permutation-only cipher is $O\left(\lceil \log_L (MN) \rceil\right)$, where MN is the size of the

image and L is the number of color intensities. They also detailed a procedure for the implementation of their attack which has $O\left(n\left(MN\right)^2\right)$ complexity, where n is the number of known/chosen plain-images. Further, Li and Lo [29] improved the implementation performance of Li et al.'s cryptanalysis by reducing its computational complexity to $O\left(n\left(MN\right)\right)$. As explained in [29], the improvement in computational complexity is obtained by employing a multi-branch tree instead of the complex intersection operations in Li et al.'s attack. Despite the good recovering performance of the Li et al.'s cryptanalysis, it is not complete and cannot precisely identify the correct elements of the input plain-images with regard to chosen-plaintext attacks. This is mainly because Li et al.'s cryptanalysis is under the assumption of a uniform distribution of all entries in the plain-image. The distribution of color intensities in most natural images is not uniform. More importantly, as explained in [28], Li et al.'s cryptanalysis can only determine a portion of the correct elements, that is, almost half of the elements, and predicts the other elements either by using image processing techniques or by inputting additional plain-images. Indeed, finding the exact value of unknown elements of an image by its partially known elements is hard.

III. Proposed Chosen-Plaintext Attack

Before we elaborate the proposed chosen-plaintext attack, the following definitions are given to describe a permutation-only image cipher.

Definition 1: Let $S = \{s | s = 0, 1, \ldots, MN-1\}$ denote the set of entry locations for an image with size $M \times N$.

Definition 2: Assume that locations of image entries are scanned in a raster order and they are enumerated by non-negative integers, which are chosen from the set of entry locations. Let $\boldsymbol{R}$ denote the matrix of entry locations, that is,

$$\boldsymbol{R} = \begin{bmatrix} 0 & 1 & \cdots & N-1 \\ N & N+1 & \cdots & 2N-1 \\ \vdots & \vdots & \vdots & \vdots \\ (M-1)N & (M-1)N+1 & \cdots & MN-1 \end{bmatrix}. \quad (1)$$

Definition 3: Let $\boldsymbol{P}$ and $\boldsymbol{C}$ denote the plain-image and cipher-image, respectively. Note that each plain-image or cipher-image is represented by an $M \times N$ matrix, where the entry of such a matrix at position s corresponds to color intensity. For any $s\,(0 \le s \le MN-1)$, let $p\,(s)$ and $c\,(s)$ be the color intensities at the position s of the plain-image and cipher-image, respectively.

Definition 4: Let X be a finite set. Permutation $\Pi_k : X \to X$ is a bijection which maps the elements of X to itself. Each secret key $k \in K$ assigns a different permutation.

Definition 5: A permutation-only image cipher ρ is defined by a permutation which, given a secret key k, maps any entry location $s\,(0 \le s \le MN-1)$ of a plain-image to its corresponding location $\rho_k\,(s)$ in the cipher-image, where ρ_k is a permutation determined by k.

The permutation-only image cipher is pseudo-random if it permutes the location of plain-image entries, with an approximate uniform probability, from the set of all possible $(\#S)!$ arrangements.

Let us now explain the procedure of the proposed chosen-plaintext attack. Deducing the permutation mapping ρ_k is equivalent to finding the secret key k. Hence, the problem of breaking the cipher is defined as an attempt to deduce the permutation mapping without any prior knowledge of the key. Consider the adversary as an oracle machine which has access to the encryption and decryption functions, that is, ρ_k and ρ_k^{-1}. The adversary asks n number of ρ_k or ρ_k^{-1} queries to obtain a set of n plain-image and cipher-image pairs, that is, $\partial = \{(\boldsymbol{P_i}, \boldsymbol{C_i})\,|i = 1, 2, \ldots, n\}$.

Proposition 1: For any $i\,(1 \le i \le n)$ and $j\,(1 \le j \le n)$, if either $\boldsymbol{P_i} = \boldsymbol{P_j}$ or $\boldsymbol{C_i} = \boldsymbol{C_j}$, then $i = j$ and pairs $(\boldsymbol{P_i}, \boldsymbol{C_i})$ and $\left(\boldsymbol{P_j}, \boldsymbol{C_j}\right)$ are identical.

Proof: This proposition is an obvious result, because the cipher is defined by a bijective permutation. ■

Definition 6: Given n pairs of plain-images and cipher-images, namely, $(\boldsymbol{P_1}, \boldsymbol{C_1}), (\boldsymbol{P_2}, \boldsymbol{C_2}), \ldots, (\boldsymbol{P_n}, \boldsymbol{C_n})$, for any pair number $r\,(1 \le r \le n)$, source location $s\,(0 \le s \le MN-1)$, target location $t\,(0 \le t \le MN-1)$, and color intensity $l\,(0 \le l \le L-1)$, where MN is the size of the image and $L-1$ is the maximum color intensity, the *equivalent set* $J_r\,(s)$ is defined as a set of target locations in the r-th cipher-image, whose values are equal to the color intensity l of the s-th location in the r-th plain-image, that is,

$$J_r\,(s) = \{t | c_r\,(t) = p_r\,(s), (0 \le t \le MN-1)\}. \quad (2)$$

Obviously, by definition, the following condition holds for the equivalent sets:

$$\bigcup_{s=0}^{MN-1} J_r\,(s) = \{t | t = 0, 1, \ldots, MN-1\}. \quad (3)$$

For any $r\,(1 \le r \le n)$, each pair of plain-images and cipher-images, that is, $(\boldsymbol{P_r}, \boldsymbol{C_r})$, involves two matrices with values assigned to entries. Consider the set S of entry locations in the plain-image. As explained in the beginning of this section, the permutation mapping ρ (see Definition 5) maps the source locations in the plain-image to the target locations in the cipher-image. To uniquely determine the permutation mapping, it is sufficient to study the arrangement of distinct entries in the pair of plain-images and cipher-images. In the case that all entries are assigned distinct values, the permutation is uniquely determined by a single pair. However, the set of color intensities, that is, $\{0, 1, \ldots, L-1\}$, is finite and the images under study may have more than L entries. Therefore, for any $r\,(1 \le r \le n)$ and $s\,(0 \le s \le MN-1)$, by the pigeonhole principle the cardinality of some equivalent sets $\#J_r\,(s)$ may not equal 1, and it is thus difficult to deduce a unique permutation mapping by knowing only one pair of plain-images and cipher-images. Hence, we need to have enough pairs of plain and cipher-images to determine the target location where each source location is mapped into. Therefore, the interest lies in using a collection of pairs, all of which have repeated values, to uniquely determine the underlying permutation. Clearly, the mapping of location s is uniquely determined if for any $s\,(0 \le s \le MN-1)$ and $r\,(1 \le r \le n)$, the equivalent sets $J_r\,(s)$ intersect in a singleton, that is,

$$\text{Source image } \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix} \xrightarrow{\text{2 digit expansion in radix 2}} \text{Expanded source image } \begin{bmatrix} 00 & 01 \\ 10 & 11 \end{bmatrix},$$

$$\text{Plain-image \#1 from bit-plane 0 } \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \xrightarrow{\text{Encryption } \rho} \text{Cipher-image \#1} \begin{bmatrix} \rho(0) & \rho(1) \\ \rho(0) & \rho(1) \end{bmatrix},$$

$$\text{Plain-image \#2 from bit-plane 1 } \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \xrightarrow{\text{Encryption } \rho} \text{Cipher-image \#2} \begin{bmatrix} \rho(0) & \rho(0) \\ \rho(1) & \rho(1) \end{bmatrix}.$$

Fig. 1. Construction procedure of the chosen plain-image/cipher-image pairs for $M = N = L = 2$.

$\bigcap_{r=1}^{n} J_r(s) = \{\rho(s)\}$, and hence it is sufficient to determine the permutation ρ if this is true for all s. Two further questions then appear:

- Is this condition sufficient to determine unique ρ?
- With what accuracy and computational cost can the mapping ρ be determined from sufficient pairs?

To answer these questions, we need to find a relationship among the number of plain-image/cipher-image pairs n, the number of locations MN and the number of assigned values in the locations L. To perform a successful chosen-plaintext attack, it is necessary to find a lower bound on the number of required pairs. However, it is possible for two given pairs to be related by a permutation on the color intensities, such that both pairs give the same information regarding possible plain-image and cipher-image locations. Thus, a useful bound on the number of required pairs will entail some restriction that avoids this possible redundancy.

A best case in connection with lower bounds on pairs can be sharply stated as follows:

Lemma 1: Given L color intensities and MN locations, for any permutation ρ, which is applied to get the respective cipher-images, there exist $n \geq \lceil \log_L (MN) \rceil$, such that ρ is uniquely determined by making use of n pairs of plain-images and cipher-images.

Proof: Consider $\lceil \log_L (MN) \rceil$ plain-images constructed by the $\lceil \log_L (MN) \rceil$ digit expansions in radix L for $s = 0, 1, \ldots, MN - 1$ in respective locations. Taken the positional digits sequentially, these values uniquely label each of the MN locations, and therefore ρ is uniquely determined by finding the target locations which exactly match the source labelling. For instance, if $M = N = L = 2$, then 2 plain-images can be constructed by 2 digit expansions in radix 2 for $s = 0, 1, 2, 3$, that is, $s' = 00, 01, 10, 11$. The construction procedure of the chosen plain-image/cipher-image pairs is depicted in Figure 1.

If fewer pairs are used, that is, $n < \lceil \log_L (MN) \rceil$, then by counting the possible sequences of L values for each location, that is $L^n < MN$, it is easy to verify that there would be less numbers than MN available locations. Thus, by the pigeonhole principle at least two locations would get the same source values in all pairs. It follows for any permutation ρ that we would be unable to distinguish between the mapped target locations. ■

We can now prove the following result.

Theorem 1: The number of required chosen plain-images n to perform a successful chosen-plaintext attack on a permutation-only image encryption algorithm is $n = \lceil \log_L (MN) \rceil$.

Proof: This theorem is an obvious result of Lemma 1. Theoretically, the permutation mapping can be easily deduced using an input matrix of size MN whose entries are sequentially labelled with distinct values $0, 1, \ldots, MN$. However, this is not practical because the encryption/decryption machine is only defined for entries of at most $L - 1$, which is usually less than the number of entries. Therefore, to make the attack feasible, the entries are firstly expanded by $\lceil \log_L (MN) \rceil$ digits with radix L. This matrix is then separated into $\lceil \log_L (MN) \rceil$ numbers of plain-images based on the digit positions in radix L. Once permutation ρ is applied to the plain-images, it produces $\lceil \log_L (MN) \rceil$ cipher-images with entries in radix L. A combination of cipher-images using the positional digits reveals the mapped locations of the original locations. ■

To illustrate the attack procedure, consider a 5×5 matrix case.

1) If $L = 1$, no further progress can be made toward determining the permutation, since the only plain-image/cipher-image pair has all entries assigned equal values.
2) If $L = 2$, then the permutation can be determined by $\lceil \log_2 (25) \rceil = 5$ pairs of plain-images/cipher-images. One way to see this is to construct an input matrix $\boldsymbol{P_1}$ with 5-bit binary expansions for the 25 locations $s = 0, 1, \ldots, 24$:

$$\boldsymbol{P_1} = \begin{bmatrix} 00000 & 00001 & 00010 & 00011 & 00100 \\ 00101 & 00110 & 00111 & 01000 & 01001 \\ 01010 & 01011 & 01100 & 01101 & 01110 \\ 01111 & 10000 & 10001 & 10010 & 10011 \\ 10100 & 10101 & 10110 & 10111 & 11000 \end{bmatrix}. \quad (4)$$

   Splitting this matrix into five binary source matrices based on bit positions, and application of the permutation ρ to these, produces five binary target matrices. When these matrices are recombined using positional bits, the mapped locations of the original locations $s = 0, 1, \ldots, 24$ will be revealed.
3) If $L = 3$, then a similar treatment requires only $\lceil \log_3 (25) \rceil = 3$ plain-image/cipher-image pairs. The original locations $s = 0, 1, \ldots, 24$, can be expanded to 3 digits in ternary representation. Hence,

$$\boldsymbol{P_2} = \begin{bmatrix} 000 & 001 & 002 & 010 & 011 \\ 012 & 020 & 021 & 022 & 100 \\ 101 & 102 & 110 & 111 & 112 \\ 120 & 121 & 122 & 200 & 201 \\ 202 & 210 & 211 & 212 & 220 \end{bmatrix}. \quad (5)$$

   Then, plain-images whose entries are 0, 1 and 2 are generated by splitting this matrix into three. Cipher-images are then generated by applying the permutation to all three plain-images. Recombining target matrices as radix 3 values gives the permuted locations of $s = 0, 1, \ldots, 24$, as required to determine the permutation.
4) Until one gets $L \leq 24$, more than one pair is necessary to deduce the permutation, as per the pigeonhole principle, some value has to be used more than once in a pair.

Next, we discuss whether it is possible to maximize the attack performance by choosing fewer than $\lceil \log_L (MN) \rceil$ pairs. This can only happen when the available pairs are well chosen. However, finding the exact minimum number of pairs to deduce permutation mapping is equivalent to the classic problem of the Test Cover [31], where a pair of a set of elements and a collection of subsets of the elements, named tests, are given. This problem is to determine the minimum sized subset of a collection of sets such that for every pair there is a test in the selection that contains exactly one of the two elements. It has been proved that finding the exact minimum sized subset is an NP-hard problem [31]. In practice, knowing the minimum set of pairs may not be as important as the accuracy of determining the permutation mapping. Indeed, the proposed approach determines the permutation mapping if there is sufficient information, and detects the lack of sufficient information when there is not.

Now we evaluate the computational complexity of the proposed chosen-plaintext attack. The first step in the attack procedure is splitting n sources from the n digit expansions in radix L of MN entry locations. The computational complexity of this step is $O(n \cdot MN)$. The second step in the attack procedure is the recombination of n target matrices as radix L values which gives the permuted locations of 0 to $MN-1$. The computational complexity of this step is also $O(n \cdot MN)$. As a result, the computational complexity of the proposed attack is $O(n \cdot MN)$. This shows that the proposed cryptanalysis is efficiently achievable by means of a limited number of chosen-plaintexts using a polynomial amount of computation time.

IV. Case Studies – Typical Permutation-Only Image/Video Ciphers

To verify the correctness of the above-discussed chosen-plaintext attack, it was tested on two typical permutation-only image/video ciphers. With respect to this, the recently proposed permutation-only image/video ciphers by Rahman et al. [16] and Fu et al. [17] are briefly overviewed, respectively.

A. Rahman et al.'s Encryption Scheme

Rahman et al.'s encryption algorithm contains two parts: a key initializing procedure and a scrambling algorithm. Using a two-dimensional Hénon map [32] described in equation (6), the key initializing procedure provides a binary sequence, which is used as a seed point to run the scrambling algorithm. The initializing procedure is briefly described as

$$\{r^n(x,y)\}_{n=0}^{1023} = \{(x_{n+1}, y_{n+1}) \mid x_{n+1} = 1 + y_n - 1.4x_n^2,\ y_{n+1} = 0.3x_n\}_{n=0}^{1023}, \quad (6)$$

$$\{b_n\}_{n=0}^{1023} = \{\sigma\left(r^n(x,y)\right)\}_{n=0}^{1023}, \quad (7)$$

where $\{r^n(x,y)\}_{n=0}^{1023}$ is the chaotic real-valued sequence generated by the Hénon map, σ is the discretization function, and $\{b_n\}_{n=0}^{1023}$ is the generated binary sequence. The chaotic binary sequence generated by the Hénon map is then used as the secret key to scramble the position of pixels in a Region Of Interest (ROI).

Algorithm 1 Rahman et al.'s Scrambling Algorithm

procedure SCRAMBLING($\boldsymbol{R}, M, N, no$)
  {Scrambling computes the encrypted ROI $\boldsymbol{R'}$ given the input ROI $\boldsymbol{R}$ and the secret key (M, N, no)}
  for $itt \leftarrow 1, no$ **do**
    $r \leftarrow 2(2M + 2N - 1) \times (itt - 1)$
    for $bnt \leftarrow 0, 1023$ **do**
      $p \leftarrow \eta + \xi \times (b_{r+0} \oplus b_{bnt}) + \varepsilon \times (b_{r+1} \oplus b_{bnt})$
      for $j \leftarrow 0, N-1$ **do**
        $\boldsymbol{R1} \leftarrow TRANS1(\boldsymbol{R})^{j,p}_{b_{r+M+j} \oplus b_{bnt}, 22.5^\circ}$
      end for
      for $i \leftarrow 0, M-1$ **do**
        $\boldsymbol{R2} \leftarrow TRANS2(\boldsymbol{R1})^{i,p}_{b_{r+i} \oplus b_{bnt}, 112.5^\circ}$
      end for
      for $k \leftarrow 0, M+N-2$ **do**
        $\boldsymbol{R3} \leftarrow TRANS3(\boldsymbol{R2})^{k,p}_{b_{r+M+N+k} \oplus b_{bnt}, 202.5^\circ}$
      end for
      for $z \leftarrow -(N-1), M-1$ **do**
        $\boldsymbol{R4} \leftarrow TRANS4(\boldsymbol{R3})^{z,p}_{b_{r+4M+4N-2+z} \oplus b_{bnt}, 292.5^\circ}$
      end for
    end for
    $\boldsymbol{R} \leftarrow \boldsymbol{R4}$
  end for
  $\boldsymbol{R'} \leftarrow \boldsymbol{R4}$
end procedure

For a ROI $\boldsymbol{R} = \{R(i,j)\}_{0 \le j \le N-1}^{0 \le i \le M-1}$ in an image $\boldsymbol{P} = \{p(i,j)\}_{0 \le j \le W-1}^{0 \le i \le H-1}$, the scrambling function employs the following four transformations to scramble $\boldsymbol{R}$ and map it to $\boldsymbol{R'} = \{R'(i,j)\}_{0 \le j \le N-1}^{0 \le i \le M-1}$, where $H \times W$ represents the size of input image and $M \times N$ denotes the size of the ROI. The relationships $M \le H$ and $N \le W$ hold in each image. The first transformation is defined as the mapping $\boldsymbol{R'} = TRANS1(\boldsymbol{R})^{j,p}_{r,22.5^\circ}$, where $0 \le j \le N-1$. This is designed to rotate each pixel in the j-th column of the ROI. If $r = 0$ then the rotation is towards the 22.5° right direction by p pixels, if $r = 1$ then the rotation is towards the 22.5° left direction by p pixels. The second transformation is defined as the mapping $\boldsymbol{R'} = TRANS2(\boldsymbol{R})^{i,p}_{r,112.5^\circ}$, where $0 \le i \le M-1$. This transformation is designed to rotate each pixel in the i-th row of the ROI. If $r = 0$ then the rotation is towards the 112.5° down direction by p pixels, if $r = 1$ then the rotation is towards the 112.5° up direction by p pixels. The third transformation is defined as the mapping $\boldsymbol{R'} = TRANS3(\boldsymbol{R})^{k,p}_{r,202.5^\circ}$, where $0 \le k \le M+N-2$. This transformation is designed to rotate each pixel at position (x, y) of ROI $\boldsymbol{R}$ satisfying $x + y = k$. If $r = 0$ then the rotation is p pixels towards the 202.5° upper-right direction, if $r = 1$ then the rotation is p pixels towards the 202.5° lower-left direction. The fourth transformation is defined as the mapping $\boldsymbol{R'} = TRANS4(\boldsymbol{R})^{k,p}_{r,292.5^\circ}$, where $1 - N \le k \le M - 1$. This is designed to rotate each pixel at position (x, y) of ROI $\boldsymbol{R}$ satisfying $x - y = k$. If $r = 0$ then the rotation is p pixels towards the 292.5° upper-left direction, if $r = 1$ then the rotation is p pixels towards the 292.5° lower-right direction. Rahman et al. used Algorithm 1 to scramble (encrypt) the data in a ROI.

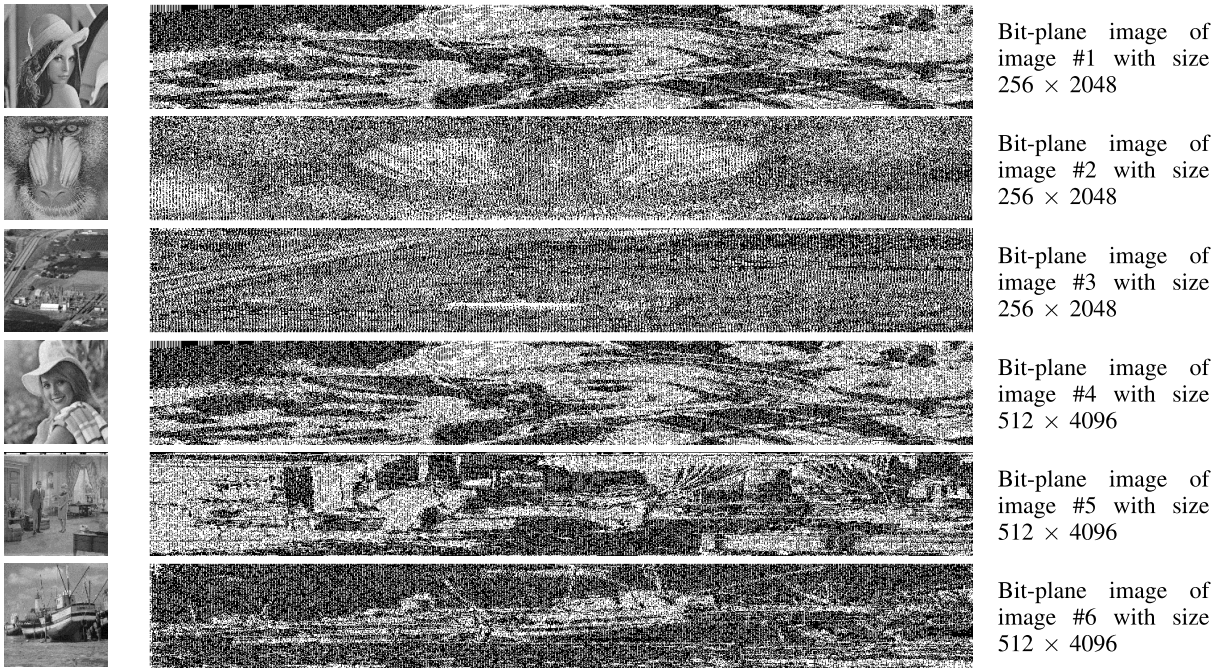

Fig. 2. Test images used in the experiments.

In fact, Rahman et al.'s scrambling algorithm is a permutation-only cipher that encrypts a plain-image by permuting the positions of all pixels in 22.5°, 112.5°, 202.5° and 292.5° degrees towards random directions. Rahman et al.'s scrambling algorithm dissipates the statistical structure of the plain-image into long range statistics. The scrambling algorithm is invertible so the de-scrambling algorithm is possible. Moreover, the scrambling algorithm is influenced by the binary sequence generated by the Hénon map, the dimension of the ROI and the control parameters such as no, η, ξ and ε.

B. Fu et al.'s Encryption Scheme

Fu et al.'s encryption algorithm is a bit-level permutation scheme, which encrypts plain-images in two iterative stages. Firstly, the plain-image is extended into a bit-plane (binary) image, which is constructed by expanding every column of the plain-image into bit-plane columns. An image of size $M \times N$ with 256 color intensities can be extended to a bit-plane image with size $M \times 8N$. In the first stage, a pseudo-random sequence is generated by a Chebyshev map, ensuring that there is no repetition, and this sequence is interpreted as the permutation mapping. A Chebyshev map is a typical invertible iterated map that generates orthogonal real-valued sequences. The Chebyshev map of degree $D\,(D = 2, 3, \ldots)$ is based on a trigonometric function defined as

$$s_{n+1} = f\,(s_n) = \cos\left(D \cos^{-1}\,(s_n)\right), \tag{8}$$

where $f : S \to S$, $S \in [-1, +1]$. To avoid the harmful effect of transitional procedure, the Chebyshev map is firstly iterated for N_0 times, where N_0 is a constant. Then, two permutation sequences of length M and $N\times$ 8 are generated, which are employed to shuffle the rows and columns of the bit-plane image, respectively. In the second stage, the shuffled bit-plane is firstly divided into eight bit-squares of equal size. Then, each bit-square is shuffled independently with different control parameters by a discretized version of Arnold Cat Map (ACM) with different control parameters. The discretized ACM is defined as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \mod N, \tag{9}$$

where N is the number of pixels in one row (or column), a and b are control parameters, x and y are pixel coordinates, and $x_n, y_n \in \{0, 1, \ldots, N-1\}$. The determinant of this map is 1; hence, it is invertible and area-preserving. This stage is iterated $m\,(1 \le m)$ rounds. Finally, both stages 1 and 2 are iterated n times. To construct the cipher image, all the 8 bit-squares are concatenated from left to right and recovered to a pixel-plane. In fact, both stages of Fu et al.'s encryption algorithm can be viewed as a one permutation stage which scrambles the entries of the bit-plane image. As explained by Fu et al. [17], the image translation to a bit-plane image and its inverse are straightforward linear transformations. Therefore, without loss of generality, we assume that Fu et al.'s algorithm encrypts bit-plane images. (s_0, D, a, b, m, n) is the secret key for Fu et al.'s encryption algorithm.

V. Experiments

According to the proposed cryptanalysis (see Section 3), the permutation mapping of the case studies, which were described in Section 4, can be easily deduced by $\lceil \log_L (MN) \rceil$ chosen plain-images. To verify this claim, numerous experiments were performed. Figure 2 depicts some of the test images which were used to perform the experiments. These test images were of size $M \times N = 256 \times 256$ and 512×512 with

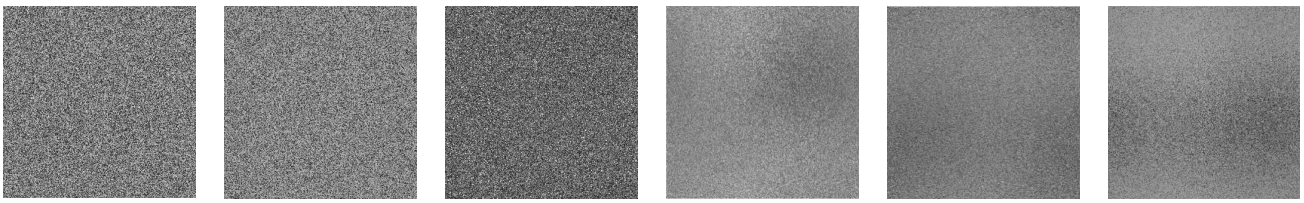

Fig. 3. Corresponding cipher-images of the six test images.

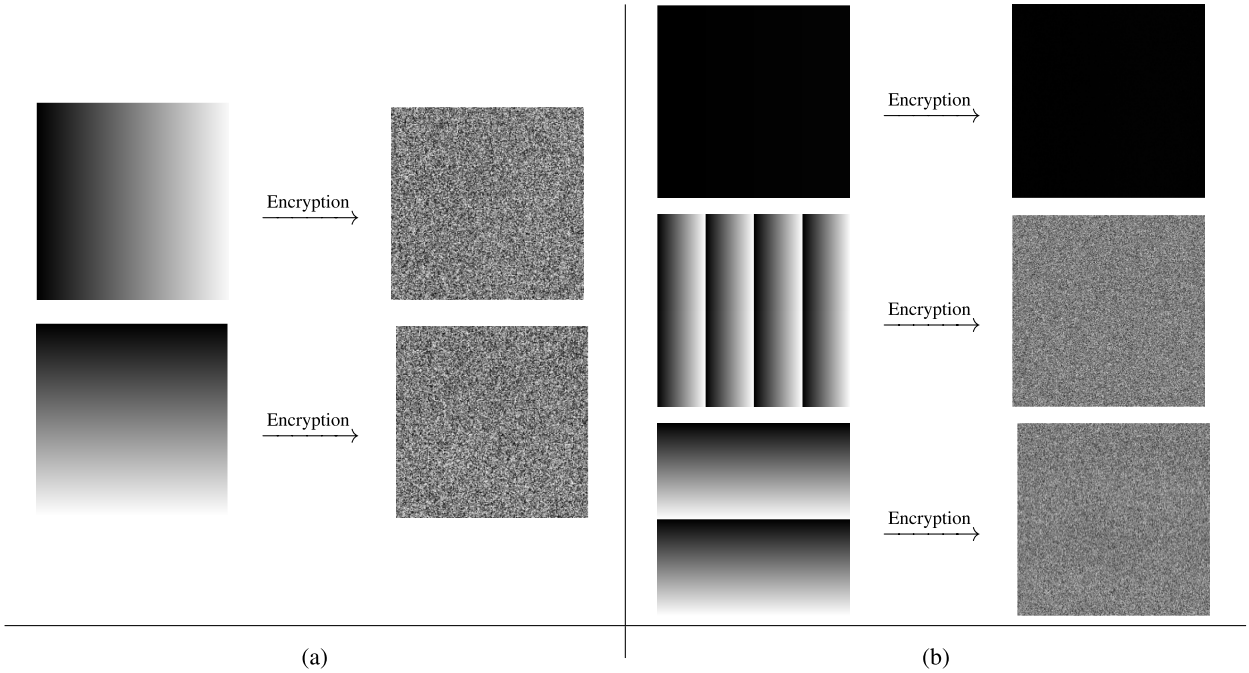

Fig. 4. Required pairs of chosen input/output images (a) with size 256×256 for finding the permutation matrix of size 256×256, and (b) with size 512×512 for finding the permutation matrix of size 512×512.

$L = 256$ color intensities. Figure 2 also depicts the bit-plane images of the test images. To deduce a unique permutation mapping, the $\lceil \log_L (MN) \rceil$ chosen plain-images were built based on the proposed coding (see Section 3). To verify the breaking performance, the corresponding cipher-images were decrypted with the inferred permutation matrices, and the recovered plain-images were compared with the original test images depicted in Figure 2. In the following subsections, the experimental results for breaking Rahman et al.'s and Fu et al.'s encryption algorithms will be given.

A. Experimental Results for Rahman et al.'s Encryption Algorithm

The test images depicted in Figure 2 were encrypted by Rahman et al.'s encryption algorithm using $(x_0, y_0) = (0.45, 0.35)$, $no = 1024$, $\eta = 1$, $\xi = 2$, and $\varepsilon = 3$ as the secret key. The corresponding cipher-images are depicted in Figure 3. According to the proposed cryptanalysis, to deduce the 256×256 permutation mapping, the adversary only requires $\lceil \log_{256} (256 \times 256) \rceil = 2$ plain-images. In addition, for 512×512 case, a similar attack procedure requires only $\lceil \log_{256} (512 \times 512) \rceil = 3$ plain-images. To deduce a unique permutation mapping, the plain-images were built based on the proposed coding (see Section 3). The chosen plain-images required for cryptanalysis and their corresponding cipher-images are depicted in Figure 4. The breaking results of cipher-images #1 and #4 are demonstrated in Figure 5.

Fig. 5. Decrypted images of the (a) cipher-image #1 and (b) cipher-image #4.

B. Experimental Results for Fu et al.'s Encryption Algorithm

The bit-plane (binary) images depicted in Figure 2 were encrypted by Fu et al.'s encryption algorithm using $(s_0, D, a, b, m, n) = (0.7, 4, 5, 2, 3, 1)$ as the secret key. The corresponding cipher bit-planes and cipher-images are depicted in Figure 6. To deduce the 256×2048 permutation mapping, the adversary only requires

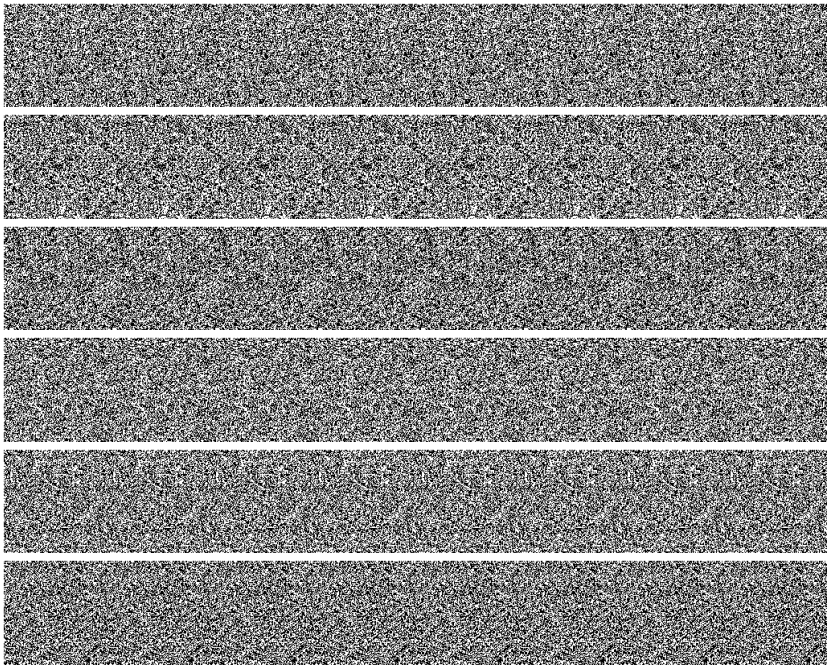

Fig. 6. Corresponding encrypted bit-plane images of the six test bit-plane images.

$\lceil \log_2 (256 \times 2048) \rceil = 19$ pairs of input/output binary images. For a 512×4096 case, a similar procedure requires only $\lceil \log_2 (512 \times 4096) \rceil = 21$ pairs of input/output binary images. To achieve a unique permutation mapping, the input images were built based on the proposed coding. The required pairs of chosen input/output binary images for obtaining the 256×2048 permutation mapping are depicted in Figure 7. Figure 7 also depicts the corresponding cipher-images constructed by the output binary images. The breaking results of cipher-images #2 and #5 are demonstrated in Figure 8.

VI. Discussion

In this section, we elaborate the advantages of our attack over the chosen-plaintext attacks of [28] and [29]. To this end, we firstly explain the general procedure that is undertaken in a chosen-plaintext attack. To successfully disclose a permutation-only cipher that works on images of size MN with L color intensities, it is sufficient to input a source image with distinct entries. However, from the practical point of view, constructing a source image with distinct entries may not be feasible, because the set of color intensities is finite and the number of entry locations usually exceeds the number of color intensities. Therefore, a collection of plain-images, all of which have repeated values, is required to uniquely determine the underlying permutation.

To disclose the underlying permutation mapping, the interest lies in utilizing a number of plain-images whose combination using the positional digits, constructs an image with distinct entries. This problem is equivalent to splitting a source image with distinct entries into a number of plain-images whose entries are equal or less than the maximum color intensity. As explained in Section 3, to split the source image, the adversary needs to expand the source entries using n digit expansions in radix L where n digits clearly produce L^n different values. This implies the following relationship for the number MN of entry locations:

$$L^n < MN \leq L^{n+1}. \tag{10}$$

The inequalities above indicate that the source entries can be expanded by $O\left(\lceil \log_L (MN) \rceil\right)$ digits, and therefore, the source image can split into $O\left(\lceil \log_L (MN) \rceil\right)$ plain-images. In other words, $O\left(\lceil \log_L (MN) \rceil\right)$ plain-images construct a source image with distinct entries. The expression $O\left(\lceil \log_L (MN) \rceil\right)$ denotes a set of functions $f(L, MN)$, such that, for sufficiently large L and MN, there exists a constant coefficient $c\,(0 < c)$ satisfying $f(L, MN) \leq c \lceil \log_L (MN) \rceil$. In this inequality, it is certain that $1 \leq c$, because n digits with radix L can produce L^n different color intensities, and if $n < \lceil \log_L (MN) \rceil$, then $L^n < MN$; and by the pigeonhole principle, at least two entries would get the same values. Therefore, $1 \leq c$.

Following the arguments above, in a known-plaintext attack, in which the plain-images are randomly selected, $c \lceil \log_L (MN) \rceil$ plain-images are required to successfully reconstruct a source image with distinct entries, where $1 \leq c$. In a chosen-plaintext attack, the aim is to find a procedure with a reduced number of required plain-images. As proved in Section 3, a tight lower bound for the required number of chosen plain-images ($c = 1$) is achieved when the MN source entries are labelled with distinct values $0, 1, \ldots, MN-1$, and then expanded by $\lceil \log_L (MN) \rceil$ digits with radix L.

To ensure the correct retrieval of the permutation mapping by using the least number of chosen plain-images, that is, $n = \lceil \log_L (MN) \rceil$, an adversary requires a precise and easy method to construct chosen plain-images. Neither [28] nor [29] proposed exact methods for the construction of the chosen

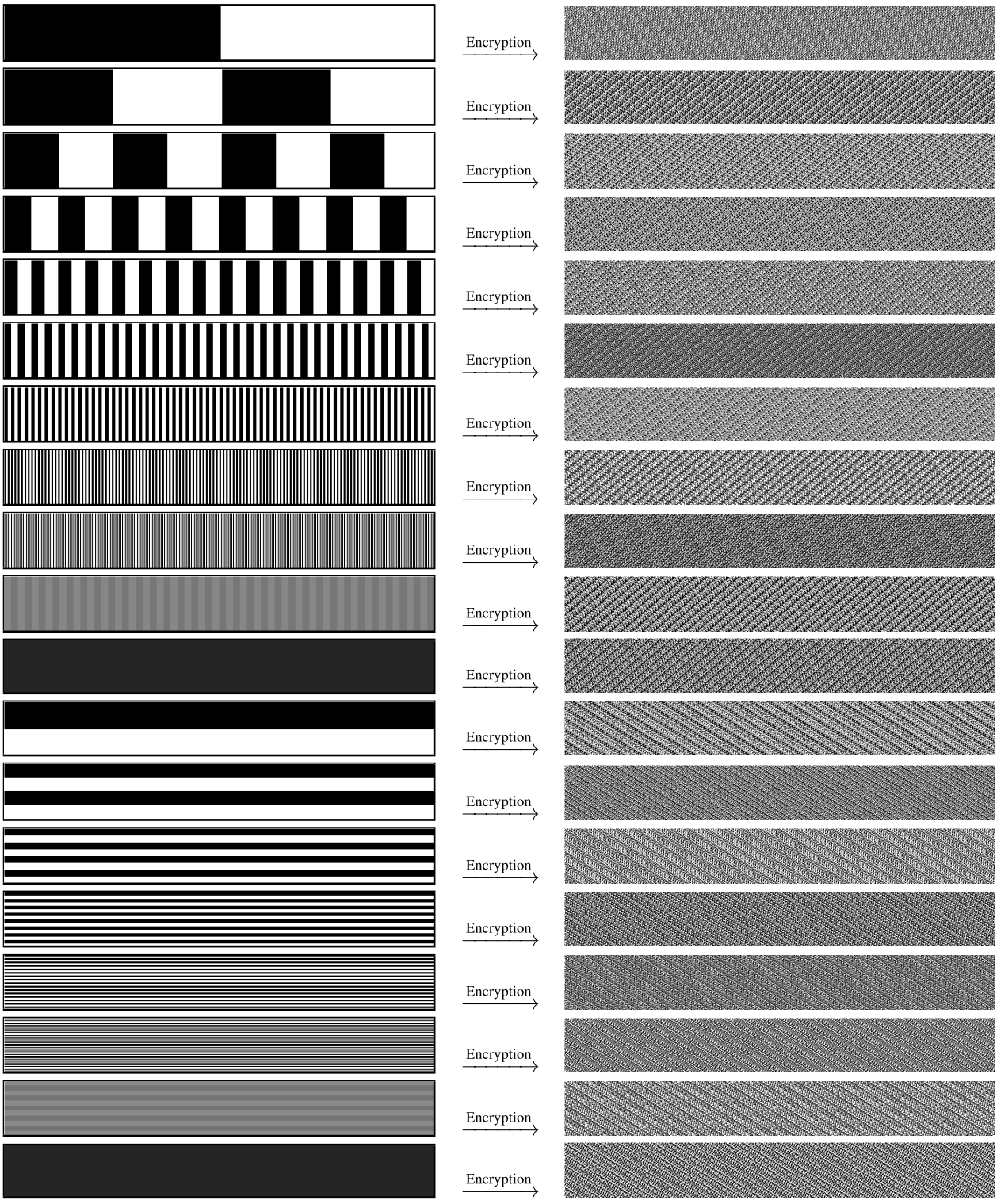

Fig. 7. Required pairs of chosen input/output bit-plane images with size 256 × 2048 for finding the permutation matrix of size 256 × 2048.

plain-images for a successful chosen-plaintext attack. In [28], Li et al. provided two rules for the construction of chosen plain-images: (1) the histogram of each chosen plain-image should be as uniform as possible; and (2) the i-dimensional ($2 \leq i \leq n$) histogram of any i chosen plain-images should be as uniform as possible. However, the rules above are not sufficiently strict, and therefore, they make a great variety of entry arrangements possible for producing chosen plain-images, which may not lead to a construction of a source image with distinct entries. Hence, Li et al.'s chosen-plaintext attack may need more plain-images compared to our chosen-plaintext attack.

(a)

(b)

Fig. 8. Decrypted images of the (a) cipher-image #2 and (b) cipher-image #5.

TABLE I
PERFORMANCE TEST

M	N	L	n	Correctly recovered elements			Run-time in seconds		
				Proposed	[28]	[29]	Proposed	[28]	[29]
87	296	23	4	100%	45%	45%	0.0158	0.7106	0.2757
1464	1134	16	6	100%	37%	37%	0.8664	68.5163	0.9052
378	1202	7	7	100%	37%	37%	0.3577	21.9006	0.3711
737	1095	28	5	100%	37.5%	37.5%	0.3532	27.8160	0.4309
153	1051	4	9	100%	35%	35%	0.1200	9.9637	0.1621
974	763	16	5	100%	35.5%	35.5%	0.3123	25.6035	0.4292
2003	1573	5	10	100%	35%	35%	2.6514	217.1524	3.1157
815	1042	3	13	100%	34%	34%	0.9435	76.1394	1.3804
517	716	3	12	100%	33%	33%	0.3882	30.6036	0.3957
1585	3061	3	15	100%	32%	32%	3.9779	501.0402	4.9172

For a better comparison, when the number n of chosen plain-images is $\lceil \log_L (MN) \rceil$, we evaluated the performance of the chosen-plaintext attacks with respect to the percentage of correctly recovered elements of the permutation matrix and the run-time. To this end, we ran 100 independent experiments with distinct M, N and L. In the performance test, we implemented the attacks using an un-optimized MATLAB code on a machine with Intel Core i7 2.5 GHz processor and 16 GB of installed memory running under Windows 7. The performance statistics for 10 experiments are reported in Table I. The experimental results confirm that compared to the chosen-plaintext attacks of [28] and [29], the proposed chosen-plaintext attack successfully recovers the complete permutation mapping with less number of chosen plain-images and less run-time.

Figure 9 depicts the curves for breaking performance of our chosen-plaintext attack and Li et al.'s cryptanalytic method [28], for a case where $M = 256$, $N = 2048$, and $L = 2$. These curves display the percentage of correctly recovered elements of the permutation matrix, with respect to the number of chosen plain-images. A comparison between the curves shows that there is a significant difference between the breaking performances of the attacks, which is mainly due to Li et al.'s criteria for constructing chosen plain-images. Indeed, Li et al.'s creation method for chosen plain-images is not precise and it cannot ensure the correct retrieval of the permutation matrix elements.

Based on the discussions above, the main advantage of the proposed attack over the chosen-plaintext attacks

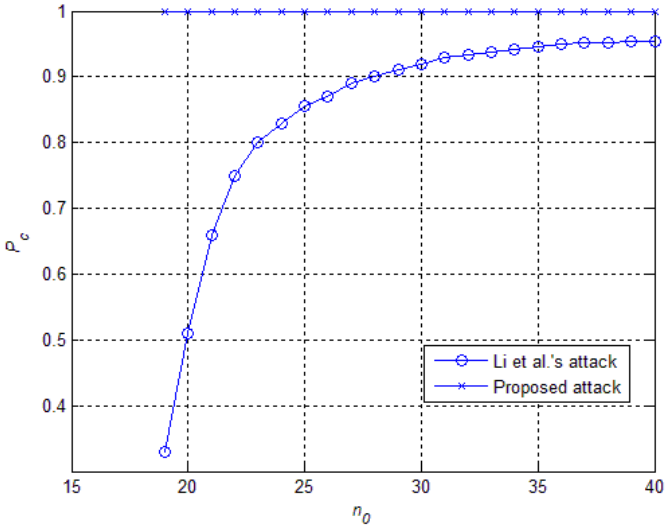

Fig. 9. Percentage of correctly recovered elements with respect to the number of chosen plain-images.

of [28] and [29] is that it presents a precise method for the construction of the chosen plain-images which ensures the correct retrieval of the permutation mapping. In addition, the proposed attack gives a tight lower bound for the number of required chosen plain-images for a successful chosen-plaintext attack. In other words, while the number of required plain-images of the chosen-plaintext attacks of [28] and [29] is an order of $\lceil \log_L (MN) \rceil$, that is, $O\left(\lceil \log_L (MN) \rceil\right)$, the number of required plain-images of the proposed chosen-plaintext attack is precisely $\lceil \log_L (MN) \rceil$. It is true that for sufficiently large MN and L, $\lceil \log_L (MN) \rceil$ (the number of plain-images that our algorithm requires) would grow as fast as any $O\left(\lceil \log_L (MN) \rceil\right)$ (the number of plain-images that [28] and [29] require); however, our chosen-plaintext attack is more accurate than Li et al.'s attack, as it provably gives the smallest number for the chosen plain-images. Furthermore, the computational complexity of Li et al.'s attack [28], Li and Lo's attack [29], and our attack are $O\left(n\,(MN)^2\right)$, $O\left(n \cdot MN\right)$ and $O\left(n \cdot MN\right)$, respectively, where n denotes the number of chosen plain-images used for a successful chosen-plaintext attack. Although the proposed chosen-plaintext attack and the chosen-plaintext attack of [29] have the same order of computational complexity, that is, $O\left(n \cdot MN\right)$, our attack is faster than that of [29], as confirmed by the results of the performance test (see the run-time comparison in Table I).

VII. CONCLUSION

In this paper, we proved that permutation-only image ciphers are completely broken against chosen-plaintext attacks. Based on the proposed attack, the permutation mapping can be easily deduced using an input matrix of size MN whose distinct entries are selected from the $\lceil \log_L (MN) \rceil$ digit expansions in radix L for $0, 1, \ldots, MN - 1$ in respective locations. In a practical attack, the number n of required chosen plain-images to break the permutation-only image encryption algorithm is $\lceil \log_L (MN) \rceil$. It has also been found that the

attack complexity is practically small, that is, $O(n \cdot MN)$. This shows that the proposed cryptanalysis is efficiently achievable by means of a limited number of chosen plain-images using a polynomial amount of computation time. Some experiments on a permutation-only image cipher have been performed to validate the performance of the proposed chosen-plaintext attack. Both theoretical and experimental results verified the feasibility of the proposed attack. From the results of this paper, it is concluded that no better pseudo-random permutations can be realized to offer a higher level of security against plaintext attacks. To offer an acceptable security level against plaintext attacks, the pseudo-random permutations should be updated to a frequency smaller than $\lceil \log_L (MN) \rceil$. In comparison with Li et al.'s, and Li and Lo's plaintext attacks, our cryptanalysis is exact, offering a lower bound on the number of required chosen plain-images and can be achieved in less computation time.

REFERENCES

[1] *Announcing the Data Encryption Standard (DES)*, NIST Standard 46-3, 1999.

[2] *Announcing the Advanced Encryption Standard (AES)*, NIST Standard 197, 2001.

[3] D. Engel, T. Stütz, and A. Uhl, "A survey on JPEG2000 encryption," *Multimedia Syst.*, vol. 15, no. 4, pp. 243–270, 2009.

[4] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol. 48, no. 8, pp. 2439–2451, Aug. 2000.

[5] D. Engel, E. Pschernig, and A. Uhl, "An analysis of lightweight encryption schemes for fingerprint images," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 173–182, Jun. 2008.

[6] X. Zhang, Y. Ren, L. Shen, Z. Qian, and G. Feng, "Compressing encrypted images with auxiliary information," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1327–1336, Aug. 2014.

[7] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the design of perceptual MPEG-video encryption algorithms," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 2, pp. 214–223, Feb. 2007.

[8] A. Pande and J. Zambreno, *Embedded Multimedia Security Systems: Algorithms and Architectures*. London, U.K.: Springer-Verlag, 2013.

[9] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, B. Furht and D. Kirovski, Eds. Boca Raton, FL, USA: CRC Press, 2004, pp. 133–167.

[10] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on selective encryption of image and video: Challenges and perspectives," *EURASIP J. Inf. Secur.*, vol. 2008, Dec. 2008, Art. ID 179290.

[11] S. Li, "Perceptual encryption of digital images and videos," in *Perceptual Digital Imaging: Methods and Applications*, vol. 14, R. Lukac, Ed. New York, NY, USA: CRC Press, 2012, pp. 431–468.

[12] R. B. Lee, "Accelerating multimedia with enhanced microprocessors," *IEEE Micro*, vol. 15, no. 2, pp. 22–32, Apr. 1995.

[13] C. Kachris, N. Bourbakis, and A. Dollas, "A reconfigurable logic-based processor for the SCAN image and video encryption algorithm," *Int. J. Parallel Prog.*, vol. 31, no. 6, pp. 489–506, 2003.

[14] Z. Dinghui, G. Qiujie, P. Yonghua, and Z. Xinghua, "Discrete chaotic encryption and decryption of digital images," in *Proc. Int. Conf. Comput. Sci. Soft. Eng.*, Wuhan, China, 2008, pp. 849–852.

[15] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 1, pp. 39–50, Jan. 2014.

[16] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, "Chaos-cryptography based privacy preservation technique for video surveillance," *Multimedia Syst.*, vol. 18, no. 2, pp. 145–155, 2012.

[17] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Opt. Commun.*, vol. 284, no. 23, pp. 5415–5423, 2011.

[18] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognit. Lett.*, vol. 31, no. 5, pp. 347–354, 2010.

[19] C. Wang, H.-B. Yu, and M. Zheng, "A DCT-based MPEG-2 transparent scrambling algorithm," *IEEE Trans. Consum. Electron.*, vol. 49, no. 4, pp. 1208–1213, Nov. 2003.

[20] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 118–129, Mar. 2003.

[21] T. Uehara and R. Safavi-Naini, "Chosen DCT coefficients attack on MPEG encryption schemes," in *Proc. IEEE Pacific-Rim Conf. Multimedia (IEEE-PCM)*, Dec. 2000, pp. 316–319.

[22] L. Zhao, A. Adhikari, D. Xiao, and K. Sakurai, "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 17, no. 8, pp. 3303–3327, 2012.

[23] X.-Y. Zhao, G. Chen, D. Zhang, X.-H. Wang, and G.-C. Dong, "Decryption of pure-position permutation algorithms," *J. Zhejiang Univ. Sci.*, vol. 5, no. 7, pp. 803–809, 2004.

[24] Y. Matias and A. Shamir, "A video scrambling technique based on space filling curves," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 293, C. Pomerance, Ed. Berlin, Germany: Springer-Verlag, 1987, pp. 398–417.

[25] M. Bertilsson, E. F. Brickell, and I. Ingemarson, "Cryptanalysis of video encryption based on space-filling curves," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 434, Berlin, Germany: Springer-Verlag, 1989, pp. 403–411.

[26] M. Kuhn. (1998). *Analysis for the Nagravision Video Scrambling Method*. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/nagra.pdf

[27] W. Li, Y. Yan, and N. Yu, "Breaking row-column shuffle based image cipher," in *Proc. 20th ACM Int. Conf. Multimedia (MM)*, New York, NY, USA, 2012, pp. 1097–1100.

[28] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Image Commun.*, vol. 23, no. 3, pp. 212–223, 2008.

[29] C. Li and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Process.*, vol. 91, no. 4, pp. 949–954, 2011.

[30] J. McCormac, *European Scrambling Systems: Circuits, Tactics and Techniques*. Dunedin, FL, USA: Waterford Press, 1996.

[31] K. M. J. De Bontridder, B. J. Lageweg, J. K. Lenstra, J. B. Orlin, and L. Stougie, "Branch-and-bound algorithms for the test cover problem," in *Proc. 10th Ann. Eur. Symp. Algorithm.*, 2002, pp. 223–233.

[32] Z. Galias and W. Tucker, "Numerical study of coexisting attractors for the Hénon map," *Int. J. Bifurcation Chaos*, vol. 23, no. 7, pp. 1–18, 2013.

Alireza Jolfaei received the bachelor's (Hons.) degree in biomedical engineering from Islamic Azad University, Tehran, Iran, in 2008, and the master's (Hons.) degree in telecommunication engineering from Imam Hossein Comprehensive University, Tehran, Iran, in 2010. He is currently pursuing the Ph.D. degree in multimedia security with Griffith University, Gold Coast, QLD, Australia.

His primary research interests include design and analysis of 3D content encryption schemes, in which his work focuses on investigating innovative solutions for maintaining the usability of encrypted content. In addition to designing usable cryptosystems, cryptanalysis is the focus of his second line of research. He has authored over 30 papers in the above-mentioned areas.

He has been awarded multiple times for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He is currently the IEEE Queensland Section Chair of Professional and Career Activities, and the Director of Equity for postgraduate students at Griffith University.

Xin-Wen Wu received the Ph.D. degree from the Chinese Academy of Sciences, Beijing, China. He was with the Chinese Academy of Sciences, University of California at San Diego, La Jolla, CA, USA, as a Postdoctoral Researcher, and the University of Melbourne, Parkville, VIC, Australia, as a Research Fellow. He was a Faculty Member with the School of Information Technology and Mathematical Science, University of Ballarat, Ballarat, VIC, Australia. He is currently a Faculty Member with the School of Information and Communication Technology, Griffith University, Gold Coast, QLD, Australia. His research interests include cyber and data security, coding techniques and information theory, and their applications. He has authored over 70 papers and book chapters and a book in the above-mentioned areas.

Vallipuram Muthukkumarasamy received the B.Sc.Eng. (Hons.) degree from the University of Peradeniya, Sri Lanka, and the Ph.D. degree from Cambridge University, Cambridge, U.K. He is currently with the School of Information and Communications Technology, Griffith University, Australia, as an Associate Professor. His current research areas include investigation of security issues in wireless networks, sensor networks, trust management in MANETs, key establishment protocols, and medical sensor networks. He established the Network Security Research Group with the Institute for Integrated and Intelligent Systems, Griffith University, and leads that Group. He has also been providing leadership to innovative learning and teaching practices as the Deputy Head of School (L&T). He has received a number of best teacher awards.