Commun Nonlinear Sci Numer Simulat 23 (2015) 294–310

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach

Jun-xin Chen [a], Zhi-liang Zhu [b,*], Chong Fu [a], Li-bo Zhang [b], Yushu Zhang [c]

[a] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China
[c] School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China

ARTICLE INFO

Article history:
Received 30 July 2014
Received in revised form 14 November 2014
Accepted 26 November 2014
Available online 4 December 2014

Keywords:
Image encryption
Chaos
Inter-pixel computing
Nonlinear pixel swapping

ABSTRACT

Recently, intrinsic image features in bit-level (e.g., higher bit-planes carry more information than lower bit-planes) have been widely accepted for building bit-level image cryptosystems. Higher bit-planes are generally handled with enhanced encryption, whereas light attention is paid to lower ones. However, the existing achievements on bit-level image features are solely based on the analyses of standard test images, and they do not hold for some special images, such as medical images. When ciphering these images, such cryptosystems may leak the important information of lower bit-planes, and other inadaptability also exists. In this paper, we firstly give out the inapplicability of the existing bit-level achievements, and then a novel chaos-based image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach is presented. Simulations and extensive security analyses demonstrate the high level of security for practical secret applications.

1. Introduction

In recent years, the dramatic developments of information and communication technologies make the multimedia information exchange across Internet easier and faster. Cryptographic approaches are therefore critical for secure image storage and distribution over public networks, especially for medical images which involve a person's privacy. However, traditional data encryption algorithms such as Triple-DES, IDEA, AES and other symmetric cryptographic algorithms are found poorly suitable for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [1].

Chaos-based cryptosystems have drawn researchers' attention due to their fundamental characteristics, such as ergodicity, sensitivity to initial condition and control parameters that can be considered analogous to the desired cryptographic properties. The permutation–diffusion architecture for chaos-based image encryption was firstly proposed by Fridrich [2] in 1998, as shown in Fig. 1. This architecture composes of two procedures, so-called the permutation and diffusion. In the first stage, pixels are shuffled by a two-dimensional area-preserving chaotic map, such as standard map, baker map and cat map. Then pixel values are modified sequentially using a quantized one-dimensional chaotic map in the diffusion stage. The Fridrich's architecture has become the most popular structure and been adopted in most of the chaos-based image cryptosystems subsequently proposed [3–31]. Based on the difference of the basic operating unit, these cryptosystems can be classified into two categories. In the first and most common type, pixel is treated as the basic operation unit and the

* Corresponding author. Fax: +86 24 86581232.
E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

http://dx.doi.org/10.1016/j.cnsns.2014.11.021
1007-5704/

encryption is performed among all the pixels of the plain image. The improvements to Fridrich's structure of this class lie in various aspects, such as novel pixel-level confusion techniques [3–9], improved diffusion schemes [10–12], integrated confusion and diffusion algorithms [13,14], combined compression and encryption mechanisms[15,16], applications of plan-image related parameters [17–20] and enhanced key stream generators [21–24,9].

On the other hand, bit is treated as the basic operating unit, and the plain image is regarded as a binary matrix in the second kind of image cryptosystems [25–30]. Image encryption algorithm at bit-level was firstly proposed in [25], and have been systematically improved by Zhang et al. in [27,29] based on some bit-level intrinsic features of plain images, such as information percentage provided by each bit [27] and the bit distribution property in microscopic and macroscopic [29]. In [27], Zhang et al. firstly proposed their viewpoint that bits at different locations carry different percentage information of the pixel. The percentage can be calculated by Eq. (1) where $i \in [0, 7]$, and is listed in Table 1.

$$p(i) = \frac{2^i}{\sum_{i=0}^{7} 2^i}. \tag{1}$$

With their equation, higher 4 bits contribute 94.125% of the total information of a pixel, whereas the lower 4 bits merely carry less than 6% of the total information. Then, Zhang et al. proposed an image encryption scheme with a bit-level permutation (BLP) [27], in which the higher four bit-planes are permutated independently, whereas the lower four bits are permutated as a group with the purpose to reduce the time consumption. In [29], researchers analyzed the intrinsic features of bit distribution of plaintexts. Based on the analysis of 12 standard test images, Zhang et al. pointed out that the total number of '0' or '1' in the plain image is almost the same with that of the cipher image, whereas the distribution of '0' or '1' is uneven in different bit-planes and is much different with that of the cipher image. Then an expand-and-shrink strategy (ES strategy) is developed to shuffle the bits among different bit-planes, and a satisfactory pixel value modification effect is subsequently achieved.

However, information percentage of different bit-planes calculated by Zhang's equation cannot necessarily reveal the actual information perceived by human eyes, especially for medical images, in which bit-planes at lower position show higher similarity with the plain image. Therefore, image encryption algorithms with enhanced attention to higher bit-planes and light concentration with lower bits may leak the significant information of lower bit-planes, and it is accordingly insecure over public networks [31]. Besides, the bit distribution property proposed in [29] is merely based on the analysis of some standard test images, and cannot be regarded as the universal feature for all gray-scale images. For example, as to medical images, there are more than 70% of the bits are '0's, much different from that of the standard test images. When confronted with medical images, the pixel modification effect of the algorithms in [27,29] downgrades remarkably. The above two viewpoints will be described in detail in Section 2, using eight medical images and eight standard test images.

In this paper, researchers firstly present the inapplicability of the existing bit-level achievements, and then we prove a lemma about the bit distribution balancing property of exclusive-OR (XOR) operation. Based on the achievement, a novel chaos-based image encryption scheme using nonlinear inter-pixel computing and swapping based permutation (NICSP) approach is developed. By launching NICSP, pixel confusion performance, bit balancing effect as well as certain image diffusion performance can be simultaneously obtained in the permutation stage. An image diffusion procedure and another NICSP are followed to construct a complete cryptosystem. The reason why an extra NICSP is padded after the image diffusion procedure lies in two aspects. (1) Through our simulations, the *NPCR* and *UACI* performance does not reach a satisfactory level such as *NPCR* > 99.60% and *UACI* > 33.4% after one round NICSP-then-diffusion encryption, and it does when another NICSP is added subsequently. (2) If opponents launch chosen-plaintext attack using a black image, the first NICSP becomes invalid immediately. In such occasion, the diffusion key stream elements can be easily revealed if the encryption is carried out one round. However, chosen-plaintext and known-plaintext attacks will be infeasible if we adopt permutation–diffusion–permutation architecture. Although the chosen-plaintext and known-plaintext attacks may outtrick the first permutation, yet the input image will be undoubtedly modified in the diffusion procedure. The resultant image is unknown and acts as the input of the second NICSP, therefore it cannot be recovered without the correct key of NICSP. Accordingly, the cryptosystem is more secure. Simulations and extensive security analyses both demonstrate that the proposed image encryption scheme has a high level of security for practical secure image applications.

Table 1
Percentage of information contributed by each bits.

Bit position	Information ratio (%)
0	0.3922
1	0.7843
2	1.5685
3	3.137
4	6.275
5	12.55
6	25.10
7	50.20