Optics and Lasers in Engineering 67 (2015) 191–204

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

An efficient image encryption scheme using gray code based permutation approach

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

[a] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China

ARTICLE INFO

Article history:
Received 27 September 2014
Received in revised form
29 November 2014
Accepted 29 November 2014

Keywords:
Image encryption
Gray code
Permutation
Pixel-related diffusion

ABSTRACT

In recent years, the operation efficiency of chaos-based image cryptosystems has drawn much more concerns. However, the workload arised from floating point arithmetic in chaotic map iteration prevents the efficiency promotion of these cryptosystems. In this paper, we present a novel image encryption scheme using Gray code based permutation approach. The new permutation strategy takes full advantage of (n, p, k)-Gray-code achievements, and is performed with high efficiency. A plain pixel-related image diffusion scheme is introduced to compose a complete cryptosystem. Simulations and extensive security analyses have been carried out and the results demonstrate the high security and operation efficiency of the proposed scheme.

1. Introduction

With the ever-increasing demand of secure image storage and transmission over public networks, efficient image encryption schemes have become increasingly attractive in recent years. However, traditional encryption algorithms, such as Triple-DES, IDEA, AES and other symmetric ciphers developed for textual information have been found not suitable for image encryption due to some intrinsic features of images such as high pixel correlation and redundancy [1]. Meanwhile, many researchers have noticed that the fundamental features of chaotic systems can be considered analogous to some ideal cryptographic properties for image encryption [2]. The properties of ergodic and high sensitivity to initial conditions and control parameters could be employed to both permutation and diffusion processes with satisfied efficiency and security [3]. In [4], Fridrich proposed a general architecture for chaos-based image cryptosystems. This architecture consists of two stages, permutation and diffusion, as shown in Fig. 1. Under this structure, a plain image is first shuffled by a two-dimensional area-preserving chaotic map so as to erase the high correlation between adjacent pixels. Then the pixel values are modified sequentially using pseudorandom key stream elements produced by a quantized chaotic map in the diffusion procedure. During the past decades or so, researchers have performed extensive analyses for this architecture, and the improvements are subsequently proposed in various aspects, such as novel pixel-level confusion approaches [5–10], permutation strategies in bit-level [11–15], improved diffusion schemes [16–18], applications of plain-image related parameters [19,20], and enhanced key stream generators [21–25]. Other techniques, such as DNA encoding [26], wavelet transform [27] and various optical approaches [28–33] are also employed to build secure image cryptosystems.

Security performance is the most important issue for image encryption. However, recent cryptanalytical works have demonstrated that some chaos-based image cryptosystems are vulnerable to various attacks, and have been successfully broken [34–40]. The most serious flaw is that the key stream completely depends on the secret key. That is, the same key stream will be used to encrypt different plain images if the secret key keeps the same. This drawback favors an attacker to launch known-plaintext or chosen-plaintext attack so as to retrieve the equivalent key stream elements and further break the whole system. Besides the security performance, speed is another important factor, as lower encryption speed will restrict their implementation for real-time applications. For chaos-based image encryption, the time consumption mainly derives from the floating point arithmetic operation and the quantization arised from the chaotic map iteration [6,41]. Therefore, when fulfilling the security requirements, how to reduce the required chaotic iteration plays critical role for efficiency promotion. In [41], an efficient diffusion mechanism using simple table lookup and swapping techniques was proposed as a light-weight replacement of chaotic iteration, while an efficient method for generating pseudorandom numbers from spatiotemporal chaos was investigated in [42]. A novel pixel swapping based image permutation approach that can contribute considerable diffusion effect was proposed in [43]. The idea is to reduce the workload of the diffusion part so that fewer overall rounds and

* Corresponding author.
E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

http://dx.doi.org/10.1016/j.optlaseng.2014.11.017
0143-8166/

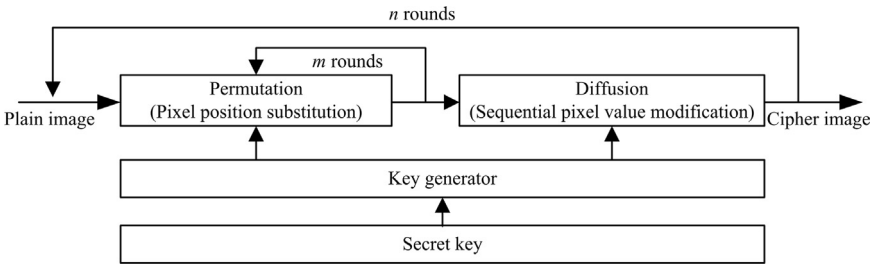

Fig. 1. The architecture of typical chaos-based image cryptosystems.

hence a shorter encryption time is needed. Similar image confusion technique that can contribute certain diffusion effect would also be found in [6]. However, there are also various weaknesses in the algorithms proposed in [6,41–43] that may downgrade the efficiency and therefore restrict their practicability for real-time secure image applications. Take the scheme in [41] as an example, if the plain image is not square or with size less than 256×256, extra chaotic mapping should be computed to ensure the table lookup diffusion procedure smoothly carried out. The computational cost is thus rising, and the encryption efficiency will be consequently downgraded.

In this paper, an efficient image encryption scheme with a Gray code based permutation approach (GCBPA) is presented. We extensively investigate the intrinsic features of a recently proposed (n, k, p)-Gray-code achievement [44], based on which the GCBPA is developed. This strategy takes full advantages of the nonlinear one-to-one correspondence between (n, k, p_1)-Gray-code and (n, k, p_2)-Gray-code. Simulations demonstrate that the GCBPA can provide comparable image shuffling effect in comparison with traditional chaos-based permutation techniques. It is well-known that Gray code can be efficiently generated using simple binary XOR and binary shift operations, and hence the GCBPA is also implemented with very high efficiency, and such is the case in our simulation. The superiority in operation efficiency allows it an outstanding alternative of the traditional image permutation strategies, such as cat map, baker map and standard map [43]. A pixel-related image diffusion approach is developed, so as to collaborate with the GCBPA for building a complete image cryptosystem. The control parameter of the introduced chaotic map is continuously perturbed according to the plain pixel value, and hence distinct key stream will be generated when ciphering different images. The known-plaintext and chosen-plaintext attacks are consequently infeasible. Simulations demonstrate that the proposed cryptosystem has a high security level and satisfactory encryption efficiency for practical secure image applications.

The remainder of this paper is organized as follows. In Section 2, the proposed image cryptosystem will be given in detail. Simulation results, the effectiveness and efficiency of the proposed scheme are reported in Section 3, whereas extensive security analyses are carried out in Section 4. Finally, conclusions will be drawn in the last section.

2. The proposed image cryptosystem

2.1. The GCBPA

2.1.1. (n, k, p)-Gray-code theory

Gray code, named after Frank Gray, generally refers to a binary-reflected code. In this code, the representations of two successive codes differ in only one bit position. Generalization of Gray codes has been systematically investigated over the last few decades [44–47]. In our scheme, (n, k, p)-Gray-code achievement in [44] (Section 2) is employed as the basis of the GCBPA. In this subsection, we briefly quote the (n, k, p)-Gray-code theory, for more details please refer to [44]

Definition 1. *The (n, k, p)-Gray-code*: Suppose that $A=(a_{k-1}, a_{k-2}, \ldots, a_1, a_0)_n$ and $G=(g_{k-1}, g_{k-2}, \ldots, g_1, g_0)_n$ are two k-digit base-n representations of the nonnegative integers sequences, respectively, i.e.,

$$A=\sum_{i=0}^{k-1} a_i n^i, \quad \text{and} \quad G=\sum_{i=0}^{k-1} g_i n^i. \tag{1}$$

G is called as the (n, k, p)-Gray-code of A if the sequences are satisfied with Eq. (2), where $0 \le i \le k-1$, $n \ge 2$, $0 \le p \le k-2$, and p represents the distance parameter.

$$g_i=\begin{cases} a_i & \text{if } i > k-p-2 \\ (a_i+a_{i+p+1}) \bmod n & \text{if } 0 \le i \le k-p-2 \end{cases}. \tag{2}$$

A more efficient conversion for software implementation of the (n, k, p)-Gray-code is given in Eq. (3), where G is the resultant Gray code, A is the original number (in binary representation), $\oplus$ represents the binary XOR operation, and $\gg$ is the binary right shift [3].

$$G=A \oplus (A \gg (p+1)). \tag{3}$$

Note that, we will use (k, d)-Gray-code in the reminder of this paper as a replacement of (n, k, p)-Gray-code, with the consideration in two aspects. (1) Base-2 Gy code is applied in our approach to represent the pixel coordinate of the original and the permutated images, and hence the parameter n is always equal to 2. Therefore, we omit this parameter in this work. (2) The word p will be used to represent the plain image, and we prefer using d as a better representation of the *distance* parameter for Gray code to clear up the potential ambiguity. In conclusion, (k, d)-Gray-code will be used in the remnants of the paper, which represents a number's k-digits Gray code with d distance.

2.1.2. The GCBPA

Now, let us investigate some interesting intrinsic features of the (k, d)-Gray-code. A definition has to be declared first.

Definition 2. *The Gray-decimal(x, k, d) function*: Suppose that x is a k-bits nonnegative integer, Gray-decimal(x, k, d) represents the decimal meaning by regarding its (k, d)-Gray-code as the standard binary representation.

Table 1 gives some (k, d)-Gray-code representations and Gray-decimal(x, k, d) outcomes of some numbers with length of 16 bit.

First, it is worth noting that the (k, d)-Gray-code of a k-bits number is also a k-bits number. As to the set of k-bits numbers x $(0 \le x \le 2^k-1)$, the transformation from x to *Gray-decimal* (x, k, d) is a bijective map, which means the map is both injective and surjective. Second, as to a special number x, *Gray-decimal*(x, k, d) function is nonlinear with x, especially for the numbers with high values. And therefore we can obtain the third property, the conversion from *Gray-decimal*(x, k, d_1) to *Gray-decimal*(x, k, d_2) is also bijective, surjective and nonlinear.

Till now, a basic (k, d)-Gray-code based permutation approach (BGCBPA) can be straightforward generated. In this