Information Sciences 264 (2014) 317–339

Contents lists available at ScienceDirect

Information Sciences

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

Design of image cipher using latin squares

Yue Wu [a,1], Yicong Zhou [b,*], Joseph P. Noonan [a], Sos Agaian [c]

[a] Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155, United States
[b] Department of Computer and Information Science, University of Macau, Macau 999078, China
[c] Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, United States

ARTICLE INFO

Article history:
Received 22 February 2013
Received in revised form 10 September 2013
Accepted 19 November 2013
Available online 27 November 2013

Keywords:
Image encryption
Latin square
Substitution–permutation network
Confusion–diffusion
Error tolerance

ABSTRACT

In this paper, we introduce a symmetric-key Latin square image cipher (LSIC) for grayscale and color image encryption. Our main contributions include (1) we propose new Latin square image encryption primitives including *Latin Square Whitening, Latin Square S-box* and *Latin Square P-box*; (2) we develop probabilistic image encryption by embedding random noise into the least significant bit-plane of images; and (3) we design a new loom-like 2D substitution–permutation network maintaining good confusion and diffusion properties with extra error tolerance. Theoretical analysis and simulation results show that the proposed method has many desired properties of a secure cipher, shows robustness against different attack models, and outperforms state of the art suggested by many peer algorithms. Open-source implementation can be found on the webpage https://sites.google.com/site/tuftsyuewu/source-code.

1. Introduction

With ubiquitous digital images and digital media devices all over the world, the importance of image security has been noticed and emphasized in recent years [50]. In the real world, digital cameras capture the real scene in the format of digital images, and are widely used in many digital devices such as smart phones, IPADs, and laptops. In the virtual world, digital images, including those taken from cameras, scanned documents or pictures, and computer-aid virtual paintings and so on, are the most common elements within a webpage besides texts on the World Wide Web. Due to extensive information within a digital image, divulged image contents sometimes cause severe problems for its owner(s). In many cases, such information leakage seriously invades personal privacy, e.g. the malicious spread of photos in personal online albums or patients' medical diagnosis images, and furthermore it may cause uncountable losses for a company or a nation, e.g. a secret product design for a company or a governmental classified scanned document.

Conventionally, digital data is encrypted by bit-stream ciphers and block ciphers [1,2,6,27]. The two well-known block ciphers are the Digital Encryption Standard (DES) [1] and its successor Advanced Encryption Standard (AES) [2]. A digital image is a specific type of digital data and can be encrypted by these conventional ciphers. However, they are somewhat insuitable for digital images because of.

- Relatively small block size: digital images are normally of several kilobits (Kb) and megabits (Mb), while conventional bit-stream/block ciphers commonly has a block size less than 256 bits.

* Corresponding author. Tel.: +853 83978458; fax: +853 28838314.
E-mail addresses: ywu03@ece.tufts.edu (Y. Wu), yicongzhou@umac.mo (Y. Zhou).
[1] Tel.: +1 6176273217; fax: +1 6176273220.

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.11.027

- Neglect of the nature of digital images: digital images are of two-dimensional data, while conventional bit-stream/block ciphers encrypt an image by indirectly encrypting a pixel sequence extracted from this image.

The first defect implies the low efficiency of encrypting a digital image using a bit-stream/block cipher [9,34,50]. The second defect implies that a pixel sequence of an image is of high information redundancy with a tilted histogram and is distinctive from a common bit sequence input to a bit-stream/block cipher. Therefore, image encryption should be adaptive to image properties and natures.

In general, digital image encryption methods can be classified into two groups: perceptual-level and bit-level. The perceptual-level image encryption methods intend to transform an image into a unrecognized one using a fast algorithm, e.g. transform techniques [8,11,53] and optical encryption techniques [12,23]. In this case, images are believed to be valuable only within a certain time period, e.g. a couple of hours. To some extend, therefore, an encrypted image by using perceptual-level image encryption is insecure because it maybe cracked after a sufficiently long time. In contrast, the bit-level image encryption aims to change an image into a random-like one. In this situation, images are believed to be valuable for a quite long time period, e.g. twenty years. Nowadays, the bit-level image encryption methods are mainly based on chaotic systems [9,17,21,28,34–36,45,46,55]. Although many existing chaotic image encryption algorithms have several good cryptographical properties, they have defects in the following aspects regardless of used chaotic systems:

- A chaotic system is defined on real numbers while a cryptosystem is defined on finite numbers.
- A chaotic system may lose its chaotic nature completely and become periodic when it is discretized.
- A chaotic system's parameters and initial values can be estimated by a number of existing tools and methods.

The first defect implies difficulties of software and hardware implementation for a chaos-based image encryption method because round-off errors in real number quantizations may lead nonreversible functions for encryption and thus make the decryption process impossible [31]. The second defect implies a chaotic image encryption method could be completely nonchaotic and thus vulnerable to attacks [20]. The third defect reveals a high risk that initial values and parameters used in a chaotic system might be fully analyzed using existing tools and methods after a long-term observation [4,5,30]. For example, [24,36] are cryptanalyzed in [20,18], respectively. Besides chaotic image encryption methods, nonchaotic image encryption methods are also researched by using various random-like patterns, e.g. cellular automata [10], P-Fibonacci transform [53], wave transmission model [21], Sudoku matrices [39,40,42,47], and Gray codes [54]. Although nonchaotic image encryption methods eliminate drawbacks of chaotic encryption methods, especially round-off errors, many of them do not have good confusion and diffusion properties [29] as in chaotic encryption methods, due to the fact that the used random-like patterns are not truly random-like.

In this paper, we introduce a novel image encryption solution LSIC. In particular, to avoid chaotic image ciphers' drawbacks like round-off errors, randomness degradations, etc. [19], LSIC is designed on integers directly; to achieve good diffusion and confusion properties, it follows the design guideline of the Markov cipher and is constructed according to the SPN [32] with all Latin-square-based primitives, including *Latin Square Whitening, Latin Square Substitution* and *Latin Square Permutation*; to achieve fast computations, it adopts a large block size of 256×256 bytes; and to further improve security, it also employs the probabilistic encryption [15,16].

The rest of this paper is organized as follows: Section 2 gives a brief review on preliminary materials. Section 3 introduces the new LSIC including its key schedule, probabilistic encryption, and Latin square based encryption primitives. Section 4 discusses simulation setups with extensive results, Section 5 analyzes the cipher security theoretically and experimentally under various attacks, and finally Section 6 concludes the paper and give discussions on open questions in the proposed LSIC.

2. Latin squares

A Latin square of order N is an $N \times N$ array filled with a set of N distinctive symbol elements, where each symbol appears exactly once in each row and each column. The name *Latin Square* is motivated by the mathematician *Leonhard Euler*, who used Latin characters as symbols.

Mathematically, we define a Latin square L of the order N by an indicator function f_L on tri-tuple (r, c, i) as follows

$$f_L(r,c,i) = \begin{cases} 1, & L(r,c) = S_i \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where r denotes the row index of an element in L with $r \in \mathbb{N} = \{0, 1, \ldots, N-1\}$; c denotes the column indx of an element in L with $c \in \mathbb{N}$; i denotes the index of a symbol element in L with $I \in \mathbf{N}$; and S_i is the ith symbol in the symbol set $\mathbb{S} = \{S_0, S_1, \ldots, S_{N-1}\}$.

Therefore, if L is a Latin square of the order N, then.

- for any fixed $c, i \in \mathbb{N}$, we have