Optik 153 (2018) 117–134

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos

Aqeel-ur-Rehman[a,b,*], Xiaofeng Liao[b], Muntazim Abbas Hahsmi[c], Rizwan Haider[d]

[a] Department of Computer Science, COMSATS Institute of Information Technology, Vehari, Pakistan
[b] Senior IEEE member, College of Electronics and Information Engineering, Southwest University, 400715, Chongqing, PR China
[c] Departments of Natural Science and Humanities, Khawaja Fareed University of Engineering and IT, RYK, Pakistan
[d] College of Computer Engineering, MID Sweden University, Jämtland, Sweden

ARTICLE INFO

Article history:
Received 14 June 2017
Accepted 25 September 2017

Keywords:
Image encryption
2D Chaotic maps
SHA-256
DNA
2-Bits substitution

ABSTRACT

In this paper, an image encryption system is proposed that uses only addition operation to achieve higher efficiency at diffusion phase after DNA encoding at pixel level. The image is first permuted and then encoded into DNA bases using sub-set of DNA complementary rules chaotically. Afterwards, the adjacent columns of DNA encoded image are added in the substitution phase named as inter-intra pixels substitution which followed by row addition named as inter-pixels substitution. This substitution is performed by adding DNA bases where each DNA base is composed of 2-bits. The addition operation performs randomly between DNA bases named mixed inter-intra pixel substitution. To strengthen security, initial conditions for chaotic maps are computed from SHA-256 hash of plain image which leads to enhance the resistance against known/chosen-plaintext and differential attacks. Due to fewer computational operations, the efficiency of the proposed cipher is high. The simulated results show that the proposed technique is extremely robust against statistical and differential attacks. It successfully surpassed the statistical tests such as Histogram, Correlation, Chi-Square and Entropy. For differential attack, it passed quantitative as well as qualitative Number of Pixel Change Rate (NPCR) and Unified Average Cipher Intensity (UACI) tests in a single round of encryption.

1. Introduction

In this era, consumers of information technology are mounting exponentially and touched a large number which cause many issues related to transmission and storage of data. Issues related with safety of data became the central topic of today's research. The integrity of digital data can be accomplished by end-to-end encryption, message authentication and several others. However, cryptography is the most important tool used to secure in an efficient manner. The elementary objective of cryptography is to transform data file into a futile file which can be transformed back if the proper keys are used. Image files do have large data capacities and it is known that high correlation between adjacent pixels, thus traditional cryptosystems,

* Corresponding author at: Department of Computer Science, COMSATS Institute of Information Technology, Vehari, Pakistan.
E-mail addresses: rehman@gmail.com, aqeel_rehman@hotmail.com (Aqeel-ur-Rehman).

https://doi.org/10.1016/j.ijleo.2017.09.099
0030-4026/

such as RSA, DES, AES, are not suitable for image encryption [1–4]. In 1998, Fridrich's proposed architecture of permutation and substitution that widely adopted to build image encryption schemes [1–5].

So for images, new cryptographic algorithms are required to develop. In most of the cases two different ways are used for encryption of images: one is optical and other is digital. Optical way is to construct physical systems depending on optics to include random information in an image [6]. Digital image encryption is most famous and convenient to manage the encryption issues because of the advantages over optical encryption which required high end devices. The chaotic map is often used in confusion and substitution phases of image encryption algorithms [7] because of its sensitivity on initial conditions [8] and efficiency.

Using chaotic maps, several of the works has been done by the researchers and the story was started from Wang et al. [9] using encryption algorithms on different blocks of image. Most of the one dimensional chaotic maps are used to obtain the pseudo-random numbers to encrypt images [10,11]. In these works, linear chaotic functions are imposed to produce the statistically effective encrypted images. A new technique of non-adjacent coupled map technique is used to encrypt the image in Ref. [12]. However, chaotic maps have outstanding features than coupled maps in case of image encryption.

Classification of chaos based image encryption schemes be contingent with the permutation approaches, manner in which diffusion is created and by a multifaceted form. Scrambling the position of plane image pixels is called *permutations* [13–16]. Several of the scientists use combined permutation, random pixel permutations, Arnold cat map scrambling and many others permutation techniques [17]. This process will not change the frequency of the image and the histogram of the image will remains unaffected. Only permutation will not save us from the statistical attacks. As permutations only change the position of the pixel values and can be reversed back by an attacker. However, the phase of substitution of image data is much more erudite than the permutation. Substitution brings us towards changing the pixel values and this change depends on the input image pixels which make us to get more secure cipher image than permutation. Using substitution only is also not a decent notion when you are dealing with high security risks. Diffusion also enables us to develop significant deviations in encryption using slight change of one pixel in the plain image [18,19]. The image encryption algorithms using either the permutation-only method or the diffusion-only method have some shortcomings in both security and speed [20]. To get the required accuracy of encryption, both of the given phases should be focused in the established algorithms.

The major problem concerned with image encryption is a passive attacker which tries to obtain the unauthorized access to the data. The security weaknesses of the algorithms are the major issue of encryption. The algorithms presented in [21–27] are broken by [28–34] using plain text images accepting same chaotic sequence of all possible permutations of the images. This type of attack is called plain text attack. Important phase of encryption algorithm is how sneakily we can use the random sequences and plain images mutually. Otherwise, same chaotic sequence applied on different images can fissure the algorithm.

In further developments, DNA became the carter for carrying image information and used to coding and decoding the pixels using chaotic maps and enforced image. Because of less number of computations, DNA technique has low power consumptions and the algorithms can be optimized [35,36]. However, DNA has high density of getting massive information of the involved image. Thus many research studies have combined DNA computing and chaotic encryption to improve the security level of chaos-based encryption algorithms [37–39].

Increasing power of DNA rule is due to several researchers who use the DNA encoding arrangement is numerous techniques to get supplementary refuge for data. Some authors use chaotic system to produce a random sequence and suggest using the DNA to get at most safety in [6,40]. In this case some encryption methods cannot be used as efficiently as they are presented. As an example Zhang et al. [41] proposed a color image cryptosystem based on DNA encoding and chaotic sequence which is wrecked by Ozakaynak et al. [42] and establish that it not work against plaintext attack.

The other important phase of security of image encryption schemes is how we choose the secret key of the algorithm. Image encryption scheme must be very sensitive to the keys used in the algorithm. Liu et al. re-examined the security of their works and established that secret key sensitivity is not sufficient for one plain-text image [43]. Moreover, in the algorithms, the encoding/decoding rules of the plain image and the key matrix are fixed [44–46]. For example, in Ref. [46], the third encoding rule is chosen and the fourth decoding rule is used; sometimes those 2 rules can be considered as a secure key to enlarge the key space. The problem can be shielded using more delicate algorithms to the convoluted key space.

In this paper, chaotic maps of multiple dimensions are utilized to incorporate high complexity as experiment results show that applying more than one chaotic map can achieve larger key space. Initial conditions required to generate sequence by coupled chaotic maps are premeditated from 256-bits hash of the plain image along with the external inputs. A new substitution mechanism is proposed named as mixed inter-intra pixel substitution in DNA mode. One of the advantages of the proposed algorithm is that it utilizes the floating-point number generated from chaotic map without conversion into integer, as conversion operation is complex and takes much time [47]. Hence, the speed of proposed system is quite satisfactory as compared to some existing algorithms [48–50]. To prove that proposed method is more effective and robust for the digital image of several categories and entrails, USC-SIPI image database is used in simulation. Using quantitative aspect of measurements and the most recent qualitative measurements security have been analyzed [6,40,50] which establish that the suggested cipher algorithm is sufficiently qualified to produce highly random types of encrypted images.

The rest of paper is organized in the following way: Section 2 gives initial condition generation method with some background of DNA rules and new way of utilization, confusion and diffusion, Section 3 considers the simulation results and