Signal Processing: *Image Communication* 42 (2016) 90–108

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

An efficient and secure cipher scheme for images confidentiality preservation

Zeinab Fawaz[a], Hassan Noura[b], Ahmed Mostefaoui[a]

[a] *FEMTO-ST Institute Disc dep, University of Franche Comte, Belfort 9000, France*
[b] *Faculty of Engineering, Lebanese University, Hadath Campus, Lebanon*

ARTICLE INFO

Article history:
Received 8 July 2015
Received in revised form
17 January 2016
Accepted 20 January 2016
Available online 30 January 2016

Keywords:
Security
Substitution
Diffusion
Image encryption
Avalanche effect
Sensitivity

ABSTRACT

In this paper, a novel image encryption scheme based on two rounds of substitution–diffusion is proposed. Two main objectives have guided the design of this scheme: (a) robustness against the most known type of attacks (statistical, chosen/known plaintext, ciphertext-only and brute force attacks) and (b) efficiency in terms of computational complexity (i.e., execution time reduction) in order to meet recent mobiles' applications' requirements. First, a dynamic key, changed for every input image is generated and used as the basis to construct the substitution and diffusion processes. Then, the encryption process is performed by the transmitter based on a non-linear S-box (substitution) and a matrix multiplication (diffusion), applied on each sub-matrix of the image. At the destination side, decryption is applied in the reverse order. We have conducted several series of experiments to evaluate the effectiveness of the proposed scheme. The obtained results validated the robustness of our scheme against all considered types of attacks and showed an improvement in terms of execution time reduction compared to the recent existed image-encryption schemes.

1. Introduction

Recent technology advances have contributed in the emerging of novel mobile multimedia applications that are able to capture, store and send multimedia data (e.g., camera glasses, smartphones, image sensors, and tablets). The profusion of such devices as well as its usage has led to a huge and voluminous production of images that are daily exchanged/shared between billions of users through social networks (e.g., Instagram, Facebook, and Twitter) or simply stored on web/cloud platforms (e.g., Apple iCloud). The popular usage of such devices has raised an urgent need to *secure the content of this personal image content*. Such a requirement is illustrated in many real situations as the one related to the recent celebrity photo hack,[1] where more than 100 individual iCloud celebrities' accounts have been hacked, making public their sensitive and private pictures (mostly naked pictures taken by their smartphones). Similar situations can also occur for ordinary people when their phones are stolen or hacked. This could be very prejudicial for those individuals, in particular in conservative countries. This security requirement is not limited to general public applications, it is also the case in several professional applications such as medical ones, where some sensitive images are required to be protected

E-mail addresses: zeinab.fawaz@univ-fcomte.fr (Z. Fawaz), hnouran@gmail.com (H. Noura), amhed.mostefaoui@univ-fcomte.fr (A. Mostefaoui).

[1] http://en.wikipedia.org/wiki/2014_celebrity_photo_hack

http://dx.doi.org/10.1016/j.image.2016.01.009
0923-5965/© 2016 Elsevier B.V. All rights reserved.

[1]. In addition, with the assistance of the cloud, mobile multimedia applications rise a new requirement/constraint that is *lower response time*; i.e., the cipher algorithm has to be as fast as possible. These two requirements have to be taken into consideration in the earlier stages of any image encryption/decryption scheme.

In general, techniques for encrypting images rely on two fundamental operations: pixel *confusion* and *diffusion*. The confusion operation aims to obscure the relationship between the cipher-text and the key. A common element to achieve the confusion property is the substitution operation. Generally, in the substitution operation, the positions of pixels are changed in order to crack the correlation between adjacent pixels of the encrypted image. In many substitution processes, pixel positions and values are changed non-linearly in order to fulfill an effective encryption scheme. On the other hand, in the diffusion operation, the pixels are changed sequentially (i.e. linear transformation) such that a small change in one pixel can affect almost all pixels of the image. Usually, substitution–diffusion operations are combined together in order to enforce the security of a cipher algorithm [2].

The main motivation of our work is to develop an approach that can fulfill the following two requirements: (a) ensuring confidentiality of the transmitted/stored image content in a robust way to protect it against attacks and (b) exhibiting a fast execution time in order to cope with the advanced demands of new devices. Obviously, there is a trade-off between these objectives. To this end, we have designed an efficient and robust approach based on a dynamic key derivation, and two rounds of dynamic substitution–diffusion processes [2] to achieve a high level of security, while ensuring a fastest time and a lower complexity compared to state-of-the-art approaches. To the best of our knowledge, our proposed scheme is the first one that deals with image encryption under both dynamic key and dynamic substitution–diffusion layers. In fact, the used key is dynamic by nature and *changes for every input image*, which makes our cipher scheme robust against the majority of known types of attacks, as confirmed by our security analysis results presented in Section 5. The main contributions of our proposal could be summarized as follows:

- *High security of image encryption*: Our cipher approach satisfies the security fundamental properties (avalanche effect, key sensitivity, randomness) with only two rounds. This is achieved, through the use of a dynamic key with a non-linear S-box (i.e., substitution) and an efficient diffusion layer.
- *Fast encryption*: The use of a dynamic key with two-rounds of substitution–diffusion processes to achieve the randomness allows the proposed approach to achieve a fast encryption speed compared to the state-of-the-art approaches [3–6].
- *Dynamic key:* The proposed encryption technique is based on the use of a dynamic key derivation. This key is generated independently from the input image and used later to encrypt the transmitted image. As a consequence, it provides a better resistance against error propagation almost observed in unreliable wireless communications and adds more randomness to the substitution–diffusion processes.
- *Good substitution–diffusion properties*: The key used for the substitution process as well as the matrix used for the diffusion process is derived from the dynamic key. Thus, it renders both processes dynamic and introduces the random-like effect to the cipher image.
- *Large key space*: The proposed image-encryption approach is based on the use of a dynamic key of size 128 which makes the brute-force attack unfeasible [7,8].
- *Real experimentation*: Rather than using a simple visual inspection test to verify the security level of the proposed approach. Extensive security tests and experiments have been implemented in order to demonstrate the robustness of our approach against the majority of known types of attacks.
- *Tailored for modern applications*: Due to its high security and fastest execution time, the proposed approach is tailored to ensure the data confidentiality in modern applications.

The rest of this paper is organized as follows: Section 2 presents the state-of-the-art of the previous work in the field of image encryption. Then, Section 3 presents the proposed cipher algorithm, by explaining its encryption and decryption schemes as well as its main processes (substitution–diffusion). Extensive performance evaluation and security analysis are studied in Sections 4 and 5, to prove the robustness of the proposed cipher against the most known types of attacks. Finally, the paper ends with a conclusion in Section 7.

2. Related work

Many encryption algorithms have been suggested in the literature. The oldest brand of cryptography begins by the use of symmetric-key standard encryption algorithms such as DES [9] and AES [10] to encrypt text forms. In fact, the situation is different in digital images, where the important is the content, and not the exact pixel value. These traditional techniques are not efficient to be used in the encryption of digital images due to the intrinsic features of images, and the strong correlation among its adjacent pixels [11]. Also, traditional encryption techniques require a long encryption time and a high computational power, which cannot fit the real-time delivery of multimedia streams [12].

Another paradigm was investigated by the researchers in the last decade, which is the “Chaos” field. Chaos consists of a non-linear dynamic system that apparently looks like random. Due to its extreme sensitivity to initial conditions, chaos was integrated extensively to build the cryptographic algorithms of digital images as in [7,13–22]. In this context, a chaos-based image encryption scheme based on bit-level permutation has been proposed in [4]. This approach is consisted of representing the image in the binary form, where each pixel is divided into 8 bits, and each bit carries a different amount of information. Then, a grouping of the same bits is performed to generate 8 different binary matrices. Then, for each binary matrix, a