J. Vis. Commun. Image R. 40 (2016) 51–57

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

On the effective subkey space of some image encryption algorithms using external key ☆

Wun-She Yap [a,b,*], Raphael C.-W. Phan [c], Bok-Min Goi [a], Wei-Chuen Yau [c], Swee-Huay Heng [b]

[a] Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Selangor, Malaysia
[b] Faculty of Information Science & Technology, Multimedia University, Melaka, Malaysia
[c] Faculty of Engineering, Multimedia University, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 14 December 2015
Revised 29 April 2016
Accepted 13 June 2016
Available online 15 June 2016

Keywords:
Image encryption
Chaos theory
Key schedule
Attacks
Key space

ABSTRACT

One of the general ways in designing a secure image encryption algorithm based on chaos theory is to derive a number of round subkeys from the `Key Schedule` algorithm under the control of an external secret key. A compulsory condition for the security of an image encryption algorithm is that the length of the external secret key should be sufficiently long in terms of bitlength. However, the sufficiently long secret key is not a guarantee that the algorithm is secure. In this paper, we emphasize the importance in designing a secure `Key Schedule` algorithm for such image based encryption techniques. Notably, we show why the effective space spanned by the subkeys should never be smaller than the external secret key space. To highlight the importance of this, we present our attacks on three recently proposed image encryption schemes.

© 2016 Elsevier Inc. All rights reserved.

1. Introduction

Block ciphers are widely used in real life applications to provide confidentiality that can protect any data transmitted between two parties through insecure channels from being leaked out to unauthorized parties. Such bulk data are encrypted using proper block cipher modes of operation recommended by the National Institute of Standards & Technology [1], such as the cipher block chaining mode, cipher feedback mode, output feedback mode and counter mode. The underlying block cipher used in the aforementioned modes of operation can be realized by any block ciphers, such as AES [2], Camellia [3], CLEFIA [4] and PRESENT [5] that appear in industry standards by such standardization bodies including ISO/IEC, ITU and IETF.

Due to increased broadband speed and wider coverage of networked personal devices, multimedia data (i.e., images, video clips and audio files) have been transmitted frequently between two parties through insecure channels. In order to protect the confidentiality [6,7] of these multimedia data, a straightforward way is to first split such data into a number of blocks and consecutively encrypt each block using a proper block cipher mode of operation. Nevertheless, some care has to be taken as to the appropriate choice of mode used for encrypting images, as Wadi and Zainal [8] showed that the plaintext image patterns in the ciphertext can still be seen when electronic codebook and output feedback modes are used to encrypt plain multimedia data as compared to cipher block chaining and cipher feedback modes.

Over the last decade, image encryption [9,10] has been proposed for secured visual communication and secured image encoding. The need for image encryption originates from the growing social awareness on the need for confidentiality and privacy due to frequent image sharing among users. To cope with the fast growing amounts of images that need to be stored, cloud-based storage becomes a natural solution for storing these images, most of which are personal and therefore relate to the privacy of users. However, due to the outsourcing of control over images to cloud storage providers, the general public remains skeptical as to whether such stored images really remain private. Thus, one of the countermeasures against personal images being illegitimately accessed is to first encrypt the images using image encryption schemes before storing the encrypted images in the cloud storage to protect the confidentiality and privacy of these images.

Chaos-based image encryption is a new research field gaining increasing interest among image security researchers, which involves chaos theory and cryptography. Different from block ciphers, chaos-based image encryption algorithms [11–19,10,20] are constructed based on chaotic maps or chaotic systems. Besides,

☆ This paper has been recommended for acceptance by M.T. Sun.

* Corresponding author at: Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Selangor, Malaysia.
E-mail addresses: yapws@utar.edu.my (W.-S. Yap), raphael@mmu.edu.my (R.C.-W. Phan), goibm@utar.edu.my (B.-M. Goi), wcyau@mmu.edu.my (W.-C. Yau), shheng@mmu.edu.my (S.-H. Heng).

http://dx.doi.org/10.1016/j.jvcir.2016.06.005
1047-3203/© 2016 Elsevier Inc. All rights reserved.

a chaos-based image encryption scheme processes an image with varying sizes while a block cipher processes an input with a fixed size. Even though many chaos-based image encryption algorithms had been proposed, a number of these had also been broken [21–28]. One of the challenging tasks that is normally neglected by the image encryption designers is the security of a `Key Schedule` algorithm. The security of an image encryption scheme will be deteriorated if the `Key Schedule` algorithm is not properly designed.

Generally, there exists two different methods in designing how a secure chaos-based image encryption scheme is to be keyed. Both methods consist of the algorithms `Encrypt` and `Decrypt`. `Encrypt` is an algorithm that takes a *secret key K* and a plain image *P* as inputs, and outputs an encrypted image *C*. Meanwhile, `Decrypt` is an algorithm that takes a secret key *K* and an encrypted image *C* as inputs, and outputs a recovered plain image *P*. Method 1 directly mixes the secret key *K* within `Encrypt` and `Decrypt`; while for Method 2 as depicted in Fig. 1, an extra `Key Schedule` algorithm is needed to generate a number of explicit *subkeys* from a given secret key *K*. Such subkeys will then be used as the effective secret key for `Encrypt` and `Decrypt`. Note that this concept of secret key *K* and subkeys derived from *K* being used as the effective key, is different from the concept of equivalent keys. More precisely, two different secret keys denoted as *K* and K' are considered as *equivalent keys* with respect to all (P, C) pairs if $C = \texttt{Encrypt}_K(P) = \texttt{Encrypt}_{K'}(P)$ for every value of *P*.

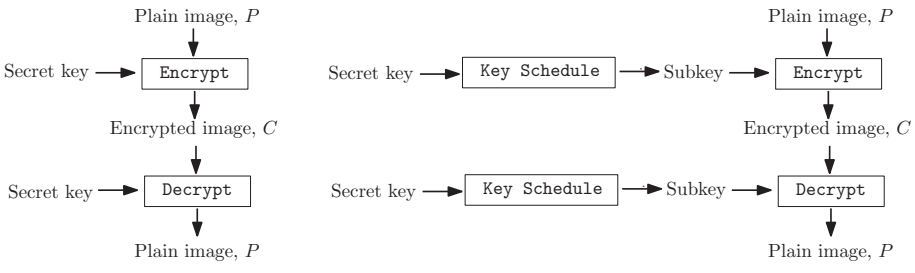
For chaos-based image encryption schemes, chaotic maps or chaotic systems are used in producing *random* chaotic sequences based on their initial conditions and the control parameters. Such a random sequence will then be exploited to encrypt a plain image. The initial conditions and the control parameters of either chaotic maps or chaotic systems are real numbers in $\mathbb{R}$ with fractional parts. In Method 1 as shown in Fig. 1, designers [12,13,15,17] treat the initial conditions and/or the control parameters of chaotic maps or chaotic systems as the secret key directly (i.e., the secret key is a real number with fractional parts). Method 2 is used especially when the external secret key is an integer in $\mathbb{Z}$ (i.e., without fractional part) where designers [14,16,20,18,19] will use such a secret key to derive the subkeys for encryption purpose (e.g., the number of rounds, the initial conditions and/or the control parameters of chaotic maps or chaotic systems) using the `Key Schedule` algorithm. Furthermore, the `Key Schedule` algorithm of an image encryption scheme may also treat the plain image related information (e.g., the number of pixels in an image or the last pixel's value of an image) as part of the input along with the external secret key. We remark that even though most of the latter type of image encryption schemes do not specifically describe their `Key Schedule` algorithms explicitly as compared to block ciphers, yet an image encryption scheme constructed using Method 2 can actually also be seen to consist of three different algorithms, i.e., `Key Schedule`, `Encrypt` and `Decrypt`.

In this paper, we focus our analysis on the `Key Schedule` algorithm without involving the study on the `Encrypt` algorithm, as the latter does not affect our security results. We term the total number of possible subkeys derived from the `Key Schedule` algorithm under the control of an external secret key as the *subkey space* and the total number of possible external secret keys as the *key space*.

As stated in [29,21,30], the secret key is the fundamental issue in all kinds of cryptosystems which include image encryption and block cipher. The security of a cryptosystem should depend only on its key and thus the selection of a key must be clearly specified and studied. The guiding rules proposed in [29,21,30] are summarised as follows:

- *Rule* IK: Avoid *invalid keys*. Such keys cause non-chaotic behaviour.
- *Rule* WK: Avoid *weak keys*. These reduce the key space.
- *Rule* RK: Guarantee the *avalanche effect* with respect to different keys. Two ciphertexts C, C' encrypted by two slightly different keys K, K' should be completely different. Otherwise these keys could be jointly brute-forced although their key spaces should be independent. In [29,21] these are called partially equivalent keys, though in security literature, such keys are better known as *related keys* [31].

To elaborate on the above, for chaos-based image encryption, the secret key must be carefully selected to avoid non-chaotic behaviour which affects the randomness properties of a chaotic sequence; such *invalid keys* [29] that do not meet this criterion should not be used. Besides, the key space should be large enough to withstand a brute-force attack. A class of *weak keys* [29,21] is such that the algorithm will behave in an unexpected way for any key belonging to this weak key class, and for which it is easy to identify whether a particular unknown secret key belongs to this class [32]. Alvarez and Li et al. [21,29] also considered the avalanche effect caused by secret keys. They suggested that two ciphertexts encrypted by two very similar keys, so-called partially equivalent keys (or also called adjacent keys in the context of chaos-based systems), should be completely different despite the keys being only slightly different, and that partial knowledge of the key should never reveal partial information about the remaining unknown part of the key. This includes the fact that the decryption should never reveal useful information to the attacker if part of the key is slowly varied. Note that the definition of partially equivalent keys i.e. very similar keys considered in [21] is different from the concept of equivalents keys discussed in the preceding paragraphs. In more detail, the former considers two similar keys (i.e. they are equal in some of their bit values), while the latter need not be similar in terms of values but cause the same encryption effect, i.e. produce the same encryption outputs. As an example of the consequence of improper secret keys, Li et al. [21]



(a) Method 1: Without `Key Schedule`

(b) Method 2: With `Key Schedule`

Fig. 1. Two methods used in keying a secure chaos-based image encryption scheme.

Download English Version:

https://daneshyari.com/en/article/528492

Download Persian Version:

https://daneshyari.com/article/528492

Daneshyari.com