Digital Signal Processing 43 (2015) 28–37

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Outsourcing chaotic selective image encryption to the cloud with steganography

Tao Xiang [a,b,*], Jia Hu [b], Jianglin Sun [b]

[a] Key Laboratory of Dependable Service Computing in Cyber Physical Society, Chongqing University, Ministry of Education, Chongqing 400044, China
[b] College of Computer Science, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Available online 11 May 2015

Keywords:
Selective encryption
Outsourcing
Cloud computing
Chaos
Steganography

ABSTRACT

This paper considers the problem where resource-limited client such as a smartphone wants to outsource chaotic selective image encryption to the cloud; meanwhile the client does not want to reveal the plain image to the cloud. A general solution is proposed with the help of steganography. The client first selects the important data to be selectively encrypted, embeds it into a cover image, and sends the stego image to the cloud for outsourced encryption; after receiving the encrypted stego image from the cloud, the client can extract the secret data in its encrypted form and get the selectively encrypted image. Theoretical analysis and extensive experiments are conducted to validate the correctness, security, and performance of the proposed scheme. It is shown that the client can fulfill the task of selective image encryption securely and save much overhead at the same time.

1. Introduction

Digital images play a fairly important role nowadays and they are everywhere, not only throughout the Internet and personal computers (PCs), but also in cellular network and smartphones. The prevalence of images facilitates our daily life greatly, but at the same time it brings security problems and challenges unprecedentedly. Image data are usually massive, multidimensional, and high-redundancy; therefore traditional encryption paradigm that treats plaintext as binary stream and encrypts on the entire bit stream is not suitable for image encryption, especially in real-time communication or resource-limited environment. For this reason, many researchers have been seeking for specific ciphers tailored for images, and chaotic image encryption is a good example [1–4]. However, the efficiency of many chaotic image ciphers is still unsatisfactory because a massive volume of data is to be handled and chaotic encryption is computationally extensive.

In this circumstance, selective encryption is proposed to only selectively encrypt a portion of important data that is crucial for visualization. Because the volume of data to be encrypted is cut down, the encryption efficiency can be boosted significantly [5–7]. Even so, selective encryption is still a heavy task for some resource-limited devices such as smartphones. Smartphones have limited hardware capability and energy supply, so that they are not able to perform complicated encryption operations, or even an orthogonal transformation being needed for many selective encryption schemes [8]. Fortunately, the emergence of cloud computing [9] provides us an effective way out to solve this problem. As the cloud has much more powerful resources, resource-limited devices can outsource selective encryption to the cloud [10].

However, outsourcing in cloud computing results in serious problems regarding security and privacy, since the data should be transmitted to the cloud and will be handled by the cloud [11,12]. The situation is even more serious in the case of outsourcing encryption because the plaintext to be encrypted is usually confidential. If the plaintext is sent to the cloud directly for encryption, the security of the plaintext can be easily compromised by the eavesdropping on communication link or the cloud. For this reason, how to let the cloud encrypt the plaintext and keep its security at the same time becomes a great challenge. Although there are many existing techniques based on homomorphic encryption [13,14] and secure multiparty computation [15,16] to allow the cloud performs computations securely, they are computationally intensive and thus not applicable for resource-limited client.

In this paper, we consider the situation in which a resource-limited client wants to outsource chaotic selective encryption of images to the cloud. The encryption consists of two phases: a permutation performed by a chaotic map and a bitwise exclusive OR (XOR) masking by another chaotic map. We propose a scheme to solve this problem with the help of steganography [17–22]. Our contributions can be summarized as follows:

* Corresponding author at: College of Computer Science, Chongqing University, Chongqing 400044, China.
E-mail address: txiang@cqu.edu.cn (T. Xiang).

http://dx.doi.org/10.1016/j.dsp.2015.05.006
1051-2004/

- To the best of our knowledge, we consider the outsourcing problem of chaotic selective encryption for the first time. We formally define the problem and make reasonable assumptions.
- We present a general solution with the help of steganography, and it guarantees that the cloud fulfills the outsourced chaotic selective encryption and has no knowledge of the plain image meanwhile.
- The proposed solution has little specific requirement on chaotic map and is thus generally suitable. Furthermore, the client can extract the embedded data in its encrypted form directly.
- Theoretical analysis and extensive experiments are conducted to validate the correctness, security, and performance of the proposed scheme. It is shown that the proposed scheme saves much computational cost than traditional local encryption and maintains satisfied security at the same time.

The rest of this paper is organized as follows. Section 2 gives the related work. Section 3 presents the problem, and some reasonable assumptions are also made there. Section 4 proposes the solution to the problem in detail. Its theoretical analyses are provided in Section 5. Experimental results are given in Section 6. Finally, Section 7 concludes the paper.

2. Related work

Various general or problem-specific theories and techniques are proposed to ensure security and privacy of outsourcing in cloud computing. We review the related work as follows.

Homomorphic encryption [13,14] is a widely explored cryptographic theory in cloud computing. It allows the cloud to carry out specific types of computations on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. For this reason, it can provide security and privacy for outsourced data computation and storage; for example, in [23], the authors proposed a homomorphic encryption method to enable direct operation over the encoded images. However, homomorphic encryption is not applicable for resource-limited clients because it is usually performed by the client side with heavy computational overhead.

Proxy re-encryption [24] is another promising way for secure data sharing in a cloud computing, as it can delegate the re-encryption capability to the proxy, such as the cloud, and re-encrypt the encrypted data by using the re-encryption key [25]. For example, in [26], a time-based proxy re-encryption scheme is proposed for secure data sharing in a cloud environment. Nevertheless, the client needs to encrypt data before outsourcing, which is usually not affordable for resource-limited clients; not even to mention the cost of key generation.

Secure multiparty computation [15,16] is also often involved in protecting data security and privacy in cloud computing, because it enables multiple parties to jointly compute a function over their inputs, while at the same time keeping these inputs private. A great number of schemes based on secure multiparty computation are proposed for privacy-assured outsourcing of image processing [27–30]. Still, secure multiparty computation is not suitable for thin clients either because all parties are supposed to be involved in the computation and the computational overhead is usually symmetry for each party.

There are some other researches on protecting images in cloud environment. In [31], traditional cryptographic techniques are used to encrypt plain images before being transmitted to the cloud. In [32], a lossy encrypted image compression method based on compressive sensing is developed for secure and effective image storage in the cloud. In [29], an image that needs to be uploaded to the cloud for template matching is masked with images obtained from social media sites and preprocessed by splitting the masked image into tiles. In [33], steganography is used to securely store images in cloud systems.

From the above review, we can find that plenty of existing work focuses on secure data storage in cloud environment, and a fundamental approach for it is to let the data owner encrypt data before outsourcing, such as homomorphic encryption and proxy re-encryption; these techniques are obviously not suitable for the scenario considered in this paper where the client is resource-limited. Secure multiparty computation supports secure computing between the client and the cloud, but the computational cost is still intensive for the client side. Although steganography [17–22] techniques are widely investigated and they are adopted in cloud system such as the work in [33], what they concerns is mainly about the data hiding during image distribution; the computation on the stego image such as encryption is not considered in existing literature.

3. Problem definition and assumptions

3.1. Problem definition

In this paper, we consider the problem in the following scenario: A resource-limited client, such as a smartphone, wants to selectively encrypt a plain image by chaotic map and distribute the encrypted image to other user. However, the client does not have sufficiently computational power or energy supply to perform the encryption involving computationally extensive iterations of chaotic map; it therefore wants to outsource the selective encryption to the cloud which has much more powerful resources, but at the same time does not want to expose the plain image to the cloud. The problem can be illustrated in Fig. 1.

3.2. Assumptions

3.2.1. The client

The client considered in this paper is a resource-limited terminal such as a smartphone. It has limited computational capability and power supply so that it cannot perform complicated calculations such as heavy encryption and signal processing, e.g. discrete cosine transform (DCT) and discrete wavelet transform (DWT). Therefore, the client can only process the image in spatial domain. The client is connected to the cloud via wireless link such as cellular network or Wi-Fi. In this circumstance, the client can only store and process images in spatial domain, i.e. pixel values; if he has the demand of image encryption, he can offload the encryption to the cloud. Even so, the client is assumed to be capable of doing lightweight encryption, say encrypting a short message such as secret key by fast stream cipher.

Fig. 1. The problem.