Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2018) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Computer Science and Computational Intelligence 2018

Permutation Modification of Reversible Data Hiding Using Difference Histogram Shifting in Encrypted Medical Image

Muhammad Fadhlan Putranto[a,*], Ari Moesriami Barmawi[a], Bambang Ari Wahyudi[a]

[a]*Telkom university, Telekomunikasi Street No. 01, Bandung, 40267, Indonesia*

Abstract

Recently, preserving the integrity of medical record, especially image medical record is important. One method for preserving the integrity is reversible data hiding (RDH) proposed by Huang et al. Reversible data hiding algorithm can recover the original image from marked image. In this paper, we implement reversible data hiding (RDH) on medical image because the correlation between the neighboring pixel can be preserved in encrypted image. In RDH, plain image is encrypted using specific encryption algorithm that consists of two processes (stream encryption algorithm and block permutation). However, since RDH used fixed block permutation, the security is weak against known plain text attack. To overcome this problem, dynamic permutation was proposed, such that the permutation would be specific for one session. In other session, different permutation would be used. Based on the experiment's result, it was shown that the security of the proposed method against known plain text attack is stronger than the previous method's one.

Keywords: Reversible Data Hiding; Difference Histogram Shifting; Encrypted Image;

1. Introduction

Due to the increasing use of internet, data security is getting important especially for preserving the integrity and the confidentiality of medical image (such as X-ray image, MRI etc.). One method for preserving the data integrity is steganography. There are several steganography methods that has been proposed, and one of them is reversible data hiding (RDH) proposed by Ni [1]. RDH is one of the data hiding technique, where the original image can be completely recovered after the embedded data have been extracted out [2]. Reversible data hiding will have benefits when true fidelity is needed, in the case of medical images. True fidelity is needed for medical image, because modifying on medical image can be deliberately dangerous or inadvertently affect the content interpretation. For example, uninten-

☆

* Corresponding author. Tel.: +62-813-1218-56900.
E-mail address: fadhlanputranto@student.telkomuniversity.ac.id

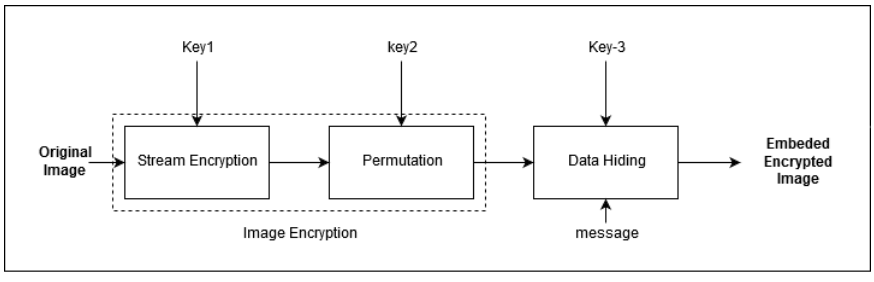
tional changes in X-ray images may cause misdiagnosis, which may result in criminal and legal offenses that could harm various parties. Therefore RDH is designed to solve the problem.

The classical RDH schemes uses three fundamental strategies: lossless compression[3], difference expansion (DE)[4], and histogram shifting (HS)[1]. In the proposed, method difference histogram shifting (DHS)[5] algorithm for data hiding is used. The proposed method used DHS because DHS has large embedding capacity and high fidelity. The main idea of this method is to explore the correlation between the neighboring pixels in a cover image. Then the additional message can be reversibly embedded into the cover image by modifying the difference histogram. It means that, the cover image can be completely recovered after message extraction. However, using this method, additional message can't be embedded into the encrypted image, because the correlation between the neighboring pixels does not exist anymore.

In this paper, we focus on preserving correlation between neighboring pixel. However, since Huang's[6] method uses static permutation (one permutation for all session), then it is easy to recover the encrypted image if the attacker has obtained the permutation for a specific session. The attacker who has access plain image and cipher image may obtain the permutation using know plain text attack. In this case, suppose the sender is the doctor and the attacker are the nurse who does not know the encryption system but she knows the plain image and can access the cipher image. In this case, she can obtain the static permutation from plain images cipher images and implement this permutation to impersonate the doctor. By implementing the permutation she can embed fake secret message into the plain image and send it to the receiver. To overcome this problem, dynamic permutation was proposed. Using dynamic permutation, the permutation for one session is different with the others. As the impact, even the attacker knows the plain image and the related cipher image of several sessions, he/she can't obtain the permutation because the permutation for one session is different with the others.

2. Huang et al. Method

Huang et al[6] proposed a new framework to preserve the correlation between neighboring pixel of an encrypted image. Huang method consisted of two sub-processes; image encryption and embedding process as shown in Fig.1(a). The encryption algorithm includes two sub-processes: stream encryption and permutation. In the stream encryption process, the plain image I is divided into N non-overlapping sub-blocks $\{B_1, B_2, \ldots, B_N\}$. The size of each sub-block is m X n and block numbering begin from the leftmost to the right blocks. This numbering method will be repeated for each row of blocks. Let $P_{i,j}(1 \le i \le N, 1 \le j \le m\ X\ n)$ denotes one of the pixels in sub-block B_i, where i represents the index of a sub-block, and j represents the index of the pixel in the sub-block B_i . In each sub-block, the pixels numbering begins from the leftmost to the right pixel. This numbering method will be repeated for each row of pixels. Furthermore, each pixel value is ex-or-ed with (*key-1*), then permuted using (*key-2*) based permutation. In data hiding process, they uses difference histogram shifting and prediction-error histogram shifting for hiding additional data to the encrypted image. Based on Huang's experiment, the receiver can decrypt the marked image and the PSNR of the marked image is 48dB.



(a)