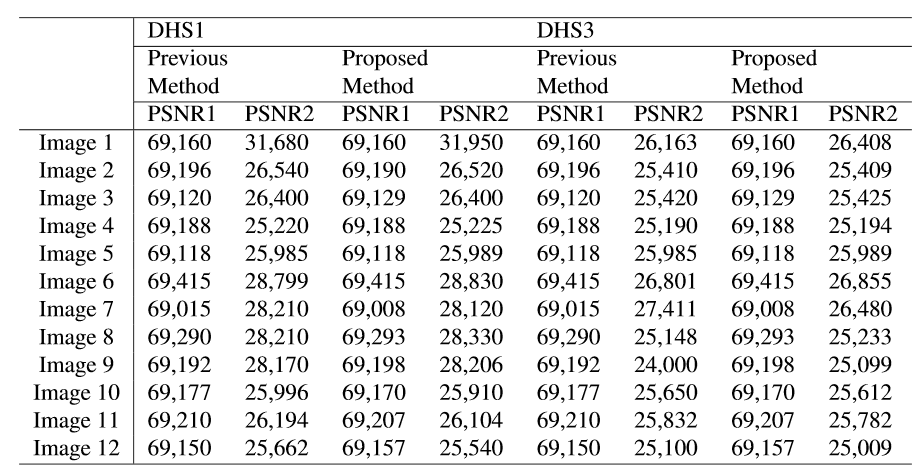
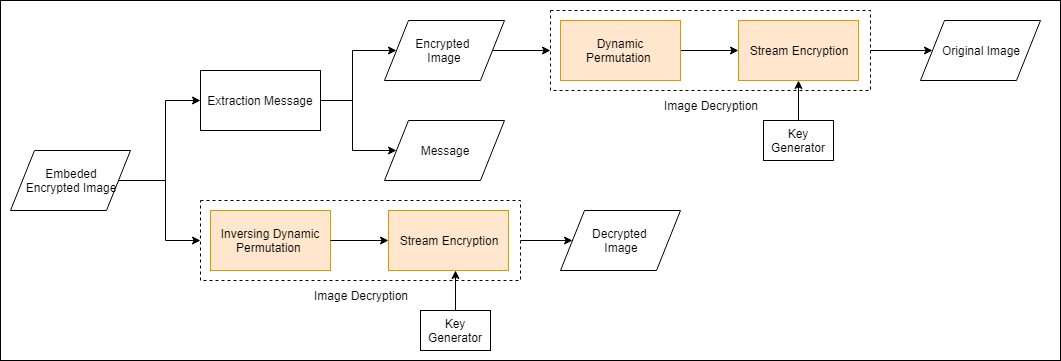
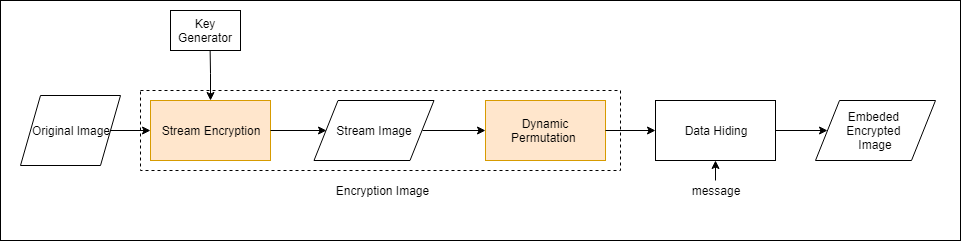
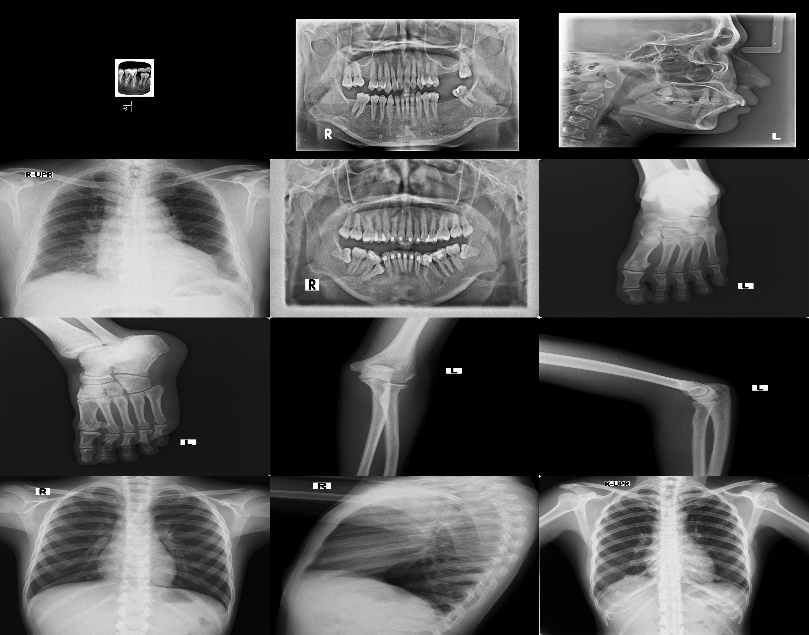


**Permutation Modification of Reversible Data Hiding Using**

**Difference Histogram Shifting in**

**Encrypted Medical Image**

** Muhammad Fadhlan Putranto Ari M Barmawi, M.Sc.,Ph.D. Bambang Ari Wahyudi, S.Kom., M.T.**

**Conclusions**

In this paper, we present RDH scheme using encryption and dynamic permutation for strengthening the security against known plain text attack. Based on the experiment result it can be concluded that the proposed method is stronger than previous one while maintaining the correlation between neighboring pixels, as well as the embedding capacity. However, in the proposed method the sender and the receiver should remember the session number before they start the session.

**Experiment and Analysis**

1. Security Analysis

To restore the original image, the attacker must restore the original arrangement of the sub-block. For obtaining the encrypted image, the attacker should find the invers of the dynamic permutation. Suppose the probability of a successful known plain text attack on an encryption system is 1/u, then using a static permutation the probability of success is 1/u. Meanwhile, when using dynamic permutations, the probability of successfully performing a known plain text attack on an encryption system would be 1/(u.N)! or 1/N! less than when using static permutations, where N is the number of sub-block. Thus, the security level of the proposed method will increase such that it is greater than the security level of Huang’s method.

1. Performance Analysis

**Dataset**

**Abstrak**

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;

**Proposed Method**