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

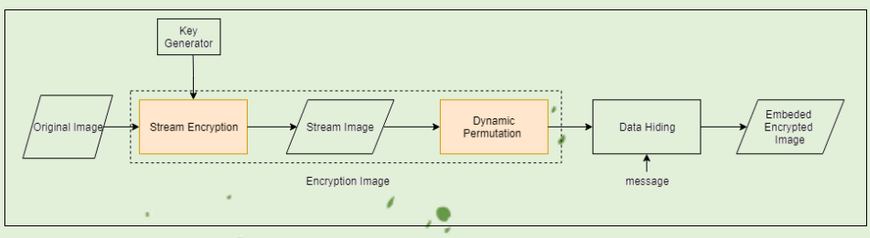
Muhammad Fadhlan Putranto **Ari M Barmawi, M.Sc.,Ph.D.** **Bambang Ari Wahyudi, S.Kom., M.T.**

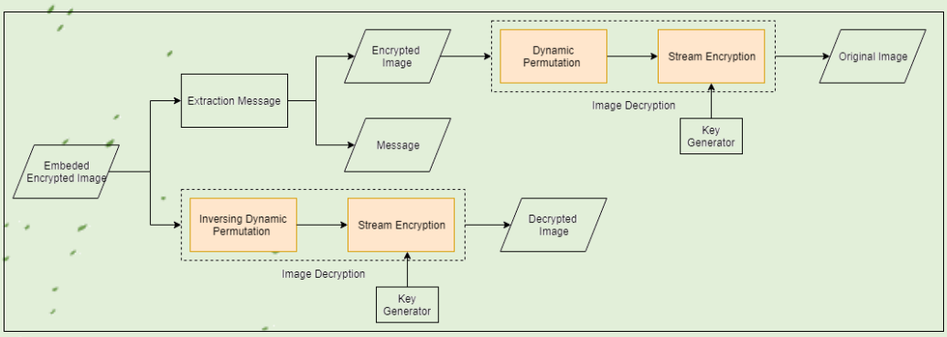
Abstrak

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.

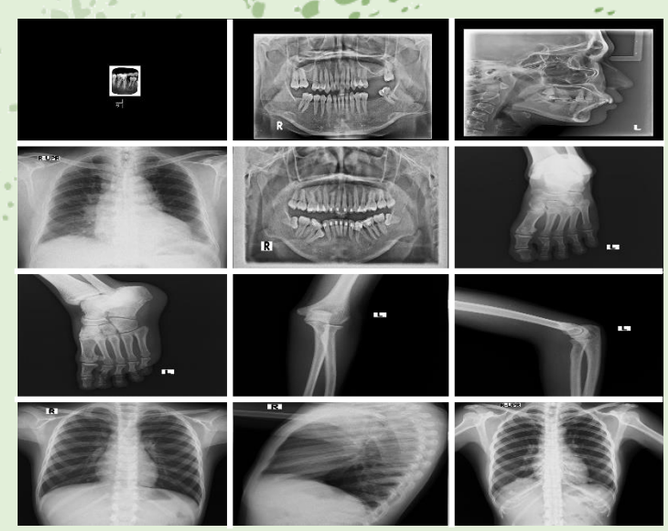
Keywords: Reversible Data Hiding; Difference Histogram Shifting; Encrypted Image;

Proposed Method





Dataset



Experiment and Analysis

A. 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.

B. Performance Analysis

	DHS1				DHS3			
	Previous Method		Proposed Method		Previous Method		Proposed Method	
	PSNR1	PSNR2	PSNR1	PSNR2	PSNR1	PSNR2	PSNR1	PSNR2
Image 1	69,160	31,680	69,160	31,950	69,160	26,163	69,160	26,408
Image 2	69,196	26,540	69,190	26,520	69,196	25,410	69,196	25,409
Image 3	69,120	26,400	69,129	26,400	69,120	25,420	69,129	25,425
Image 4	69,188	25,220	69,188	25,225	69,188	25,190	69,188	25,194
Image 5	69,118	25,985	69,118	25,989	69,118	25,985	69,118	25,989
Image 6	69,415	28,799	69,415	28,830	69,415	26,801	69,415	26,855
Image 7	69,015	28,210	69,008	28,120	69,015	27,411	69,008	26,480
Image 8	69,290	28,210	69,293	28,330	69,290	25,148	69,293	25,233
Image 9	69,192	28,170	69,198	28,206	69,192	24,000	69,198	25,099
Image 10	69,177	25,996	69,170	25,910	69,177	25,650	69,170	25,612
Image 11	69,210	26,194	69,207	26,104	69,210	25,832	69,207	25,782
Image 12	69,150	25,662	69,157	25,540	69,150	25,100	69,157	25,009

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.