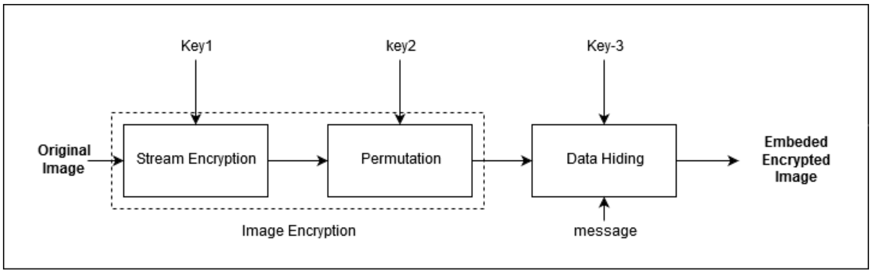
tional changes in X-ray images may cause misdiagnosis, which may result in criminal and legal offenses that could harm various parties. Therefore RDH is designed to solve the problem.

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 $P_{i,j}(1 \leq i \leq N, 1 \leq j \leq m\ X\ n)$ 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)

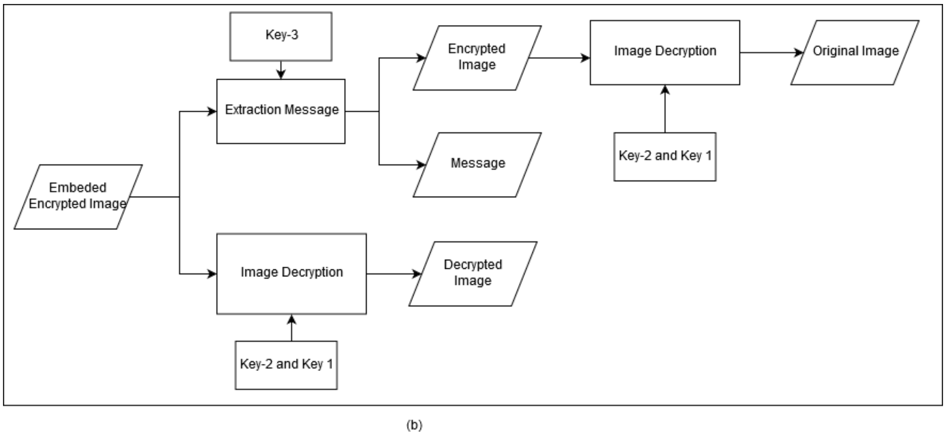


Fig. 1: Block Diagram of Huang et al a) Data hiding process b) Data extraction and image restoration

## 3. Proposed Method

The proposed method consisted of two processes, embedding (Fig.2 ) and extracting method (Fig.3). Embedding method consisted of two process, image encryption and data hiding, while extracting method consisted of data extraction and image recovery processes. In the proposed method, Huang's method is used for image encryption, but with modification in permutation process, by implementing dynamic permutation to scramble all sub-blocks in encrypted medical image. Dynamic permutation is a permutation based on polynomial congruence, such that for each session with the same receiver a unique key is applied.

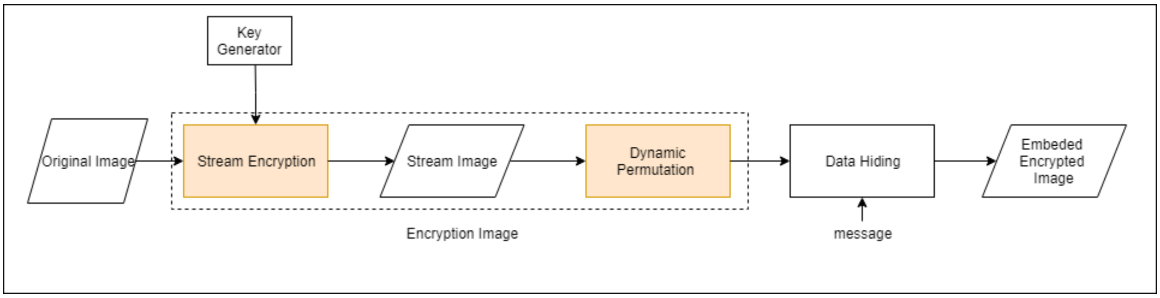


Fig. 2: Embedding process of the proposed method

### 3.1. Embedding

The embedding process consisted of two processes i.e. image encryption and data hiding, as shown in Fig.2. Since the correlation between neighboring pixel should be preserved after image encryption, we could implement RDH independently, such that the receiver may either decrypt the encrypted image without extracting the embedded message, or decrypt the encrypted image after extracting the embedded message.

#### 3.1.1. Image Encryption Algorithm

The encryption algorithm consisted of two processes, i.e. specific stream encryption and permutation. For preserving the correlation between neighboring pixel after image encryption, Huang's stream encryption was used. In encryption process, the cover image $I$ was divided into $N$ non-overlapping sub-blocks ( $B_1, B_2, \ldots, B_N$ ). The sub-blocks size used in this research is *3 x 3* and block numbering begins from the leftmost to the right blocks. Then, we have $N$ sub-block with 9 pixels in each sub-block. Let $P_{i,j}(1 \leq i \leq N, 1 \leq j \leq 9)$ denotes pixel value of $j^{th}$ pixel 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 $B_i$.