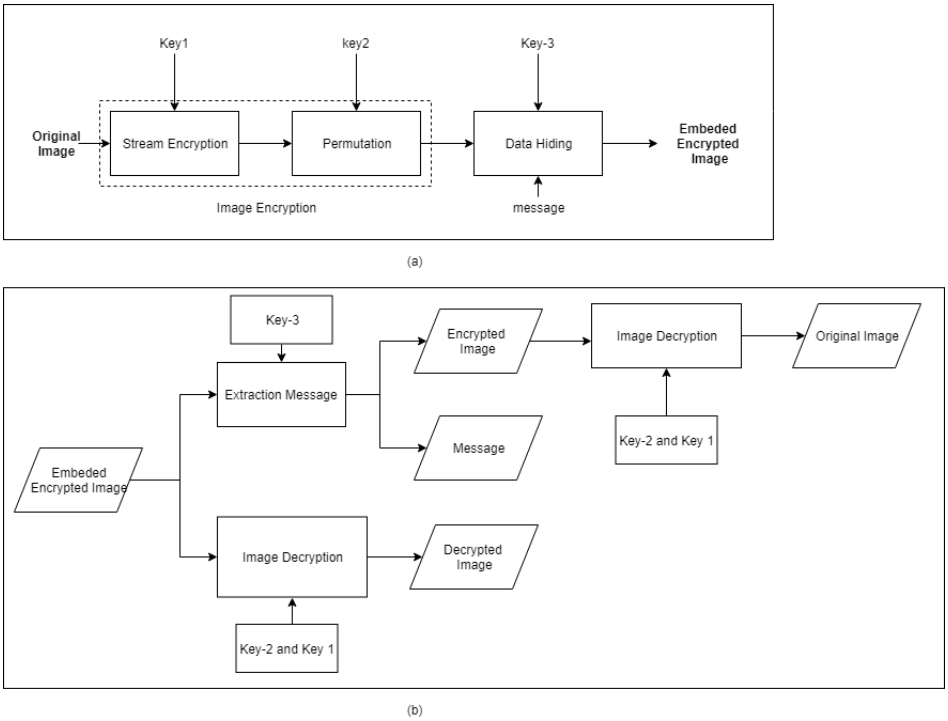
2. Studi Terkait



Gambar 1. Blok Diagram dari *Huang, Shi* a) Proses *data hiding* b) Ekstraksi pesan dan restorasi gambar

Huang, Shi [2] mengusulkan algoritma baru untuk menjaga korelasi antara piksel tetangga dari gambar terenkripsi. Metode *Huang, Shi* terdiri dari dua sub-proses; enkripsi gambar dan proses penyisipan seperti yang ditunjukkan pada Gambar 1(a). Algoritma enkripsi mencakup dua sub-proses: *stream encryption* dan permutasi. Pada proses *stream encryption*, *plain image I* dibagi menjadi N subblok yang tidak saling tumpang tindih (*non overlapping*) $\{B_1, B_2, \ldots, B_N\}$. Ukuran setiap sub-blok adalah $m \; X \; n$ dan penomoran blok dimulai dari blok paling kiri ke kanan. Metode penomoran ini akan diulang untuk setiap baris blok. Didefinisikan $P_{i,j}$ ($1 \leq i \leq N$, $1 \leq j \leq m \; X \; n$) merupakan salah satu piksel dalam sub-blok B_i, dimana i adalah indeks sub-blok, dan j adalah indeks dari pixel disub-blok B_i. Disetiap sub-blok, penomoran piksel dimulai dari paling kiri ke piksel kanan. Metode penomoran ini akan diulang untuk setiap baris piksel di dalam sub-blok. Selain itu, setiap nilai piksel di *ex-or* dengan (*key-1*), kemudian permutasi menggunakan (*key-2*). Dalam proses penyisipan data, mereka menggunakan *difference histogram shiffting* dan *prediction-error histogram shifting* untuk menyembunyikan data ke gambar yang dienkripsi. Berdasarkan percobaan *Huang, Shi*, penerima dapat mendekripsi gambar yang ditandai dan PSNR dari gambar yang ditandai adalah 48dB.

3. Sistem yang Dibangun

Metode yang diusulkan terdiri dari dua proses, penyisipan (*embedding*) (gambar 2) dan ekstraksi (gambar 3). Metode penyisipan terdiri dari dua proses, yakni enkripsi gambar dan penyembunyian data, sedangkan metode ekstraksi terdiri dari ekstraksi data dan proses pemulihan gambar. Pada penelitian ini, kami menggunakan metode *Huang, Shi* dalam melakukan enkripsi gambar, tetapi dengan modifikasi pada proses permutasi dengan menerapkan permutasi dinamis untuk mengacak semua sub-blok dalam gambar medis yang terenkripsi. Permutasi dinamis adalah permutasi berdasarkan kongruensi polinomial sehingga setiap gambar memiliki pola permutasi yang berbeda.