# BAB I PENDAHULUAN

## Latar Belakang

*S-boxes* adalah salah satu struktur paling dasar yang digunakan dalam algoritma enkripsi blok. Struktur *s-boxes* dalam algoritma enkripsi digunakan untuk operasi perubahan *byte* (Wang et al., 2019). *S-boxes* utamanya dimaksudkan untuk memperkenalkan sifat nonlinier dalam algoritma enkripsi, sehingga membuatnya tahan terhadap kriptanalisis linier dan diferensial (Ahmad & Chopra.,2018). *S-boxes* adalah komponen inti dan telah banyak digunakan di hampir semua sistem kriptografi blok konvensional atau tradisional, seperti *Data Encryption Standard* (DES) dan *Advanced Encryption Standard* (AES) (Wang, et al., 2009). Namun, pada penelitian yang dilakukan oleh Liu et al, tentang penggunaan *s-boxes* tradisional memiliki banyak kelemahan jika digunakan pada citra seperti tingginya korelasi antara piksel yang berdekatan, redundansi, dan format penyimpanan khusus dalam gambar. Untuk itu *chaotic system* yang nonlinier dan beberapa karakteristiknya seperti ergodisitas, determinan, dan sensitifitas tinggi terhadap kondisi awal menjadikannya *pseudorandom* dan ketidakpastian, membuat *chaotic system* cocok untuk enkripsi gambar (Liu, et al., 2015). **Banyak penelitian enkripsi dengan mengkombinasikan *s-boxes* dan *chaotic system***  salah satunya pada tahun 2010, Özkaynak dan Özer menggunakan *chaos* dan *s-boxes.*

Beberapa penelitian enkripsi dengan *s-boxes* telah dilakukan diantaranya pada tahun 2014, Wang dan Qian mengkombinasikan *Dynamic S-boxes* dan *Chaotic system*. Algoritma ini mengamankan citra dengan *s-box* yang dibangun oleh *chaotic system* dengan kunci 256 bit yang akan digunakan untuk menghasilkan parameter dan keadaan awal *chaotic system* untuk *s-box* pertama. Kemudian *plain image* dibagi ke dalam kelompok di mana piksel digantikan oleh *s-boxes* dan untuk menghancurkan korelasi piksel yang berdekatan, gambar akan dikelompokkan dalam empat arah (Wang & Qian., 2014). Algoritma yang diterapkan oleh Wang dan Qian memiliki kelemahan yaitu, dalam melakukan enkripsi membutuhkan waktu yang cukup lama, ruang kunci yang dimiliki cukup kecil dan hanya memproses citra *grayscale*. Pada tahun 2016, Devaraj dan Kavitha melakukan penelitian dengan mengkombinasikan *Dynamic S-boxes* dan *Modified Standard Map*. Algoritma yang diusulkan memiliki tingkat kecepatan enkripsi lebih cepat, ruang kunci yang besar dan diterapkan untuk citra berwarna. Teknik enkripsi dilakukan terdiri dari dua bagian, pertama *confusion* dengan *permutation* *pixel* dan *dynamic s-boxes* untuk mengacak gambar. Kedua memodifikasi nilai *pixel* dan *diffusion* dilakukan dengan pola acak. Dan urutan kunci kacau dihasilkan dengan menggunakan *modified standard map* (Devaraj & Kavitha., 2016).

Citra yang telah diamankan menggunakan kombinasi rangkaian *s-boxes* akan menghasilkan citra acak yang dapat menimbulkan kecurigan bagi pihak lain. Untuk mengatasi hal ini maka dilakukan penyembunyian citra kedalam sebuah media dengan teknik steganografi. Steganografi *Least Significant Bit* (LSB) adalah salah satu teknik di mana bit yang paling tidak signifikan dari gambar diganti dengan bit data (Barhoom & Abo.,2015). Kelemahan steganografi menggunakan LSB yaitu penyusup mudah mengubah semua *pixel* gambar kemudian merekonstruksinya untuk mendapatkan informasi yang tersimpan di LSB (Joshi et al, 2013). Untuk meningkatkan kapasitas penyimpanan pesan rahasia, tahun 2015 Bhalshanskar dan Gulve merancang algoritma modifikasi LSB dengan *range of bytes* dan struktur piramida. Hal ini dilakukan dengan cara menyembunyikan bit-bit rahasia secara acak di *byte* piramida (Bhalshanskar dan Gulve, 2015).

Berdasarkan uraian di atas, maka topik ini diangkat sebagai tugas akhir dengan judul **“Pengamanan Citra Warna Menggunakan Dynamic S-Boxes dan LSB ROB dengan Struktur Piramida”.**

## Rumusan Masalah

Berdasarkan pada uraian latar belakang di atas, maka yang menjadi permasalahan sehingga perlu dilakukan penelitian ini adalah bagaimana tingkat ke-acakan bit dan sensitivitas kunci pada citra rahasia setelah proses enkripsi dengan menggunakan kombinasi algoritma *Dynamic S-Boxes* dan *Modified Standard Map*.

## Tujuan

Tujuan dari tugas akhir ini adalah :

1. Membangun aplikasi untuk pengamanan citra dengan menggunakan kriptografi *Dynamic S-Boxes* dan LSB ROB dengan Struktur Piramida untuk menghindari terjadinya pencurian dan pemalsuan data gambar
2. Mengetahui tingkat keamanan dari sistem yang dibangun dengan kriptografi *Dynamic S-Boxes* terhadap sensitivitas kunci rahasia terhadap kualitas *stego images*.

## Manfaat

1. Sistem yang dibuat ini dapat digunakan sebagai alternatif pengamanan citra
2. Sistem ini dapat dijadikan sebagai referensi untuk pengembangan sistem kemananan citra lebih lanjut

## Batasan Masalah

Batasan masalah dari tugas akhir ini, antara lain :

* 1. Citra asli yang dapat digunakan sebagai masukan merupakan citra RGB 24 bit dengan format .bmp
  2. Citra yang akan diamankan merupakan citra persegi dengan ukuran minimal 50 x 50 *pixe*l dan maksimal 200 x 200 *pixel*.

## Metodologi Penelitian

Metodologi yang digunakan dalam penyusunan tugas akhir ini adalah sebagai berikut :

1. Mempelajari referensi

Pada tahap ini membaca dan mempelajari referensi yang ada, agar dapat memahami proses kerja dari metode yang digunakan pada tugas akhir.

1. Membuat aplikasi dengan model *waterfall*
   1. Analisis kebutuhan

Pada tahap ini dilakukan analisis kebutuhan fungsional menggunakan *use case diagram*, kebutuhan *non-*fungsional memanfaatkan PIECES dan *Flow Chart* dalam proses sistem

* 1. Perancangan

Merancang *user interface* perangkat lunak yang akan dibuat menggunakan *Balsamic Mockup*

* 1. Penulisan program

Melakukan penulisan kode program berbasis desktop menggunakan C#.net

* 1. Pengujian

Dalam pengujian kualitas citra dengan perhitungan *Peak Signal-to-Noise Ratio* (PSNR). Adapun pengujian yang dilakukan yaitu pengaruh panjang kunci terhadap kualitas citra

1. Menarik kesimpulan dari hasil pengujian
2. Menyusun laporan Tugas Akhir.