BAB I
PENDAHULUAN

1.1. Latar Belakang

Kriptografi visual pertama kali diperkenalkan oleh Naor dan Shamir pada tahun 1995, dimana proses enkripsi dilakukan dengan membagi citra menjadi beberapa citra acak yang ditampilkan dalam bentuk transparansi dinamakan *shares* dan dapat direkonstruksi dengan menggunakan sistem visual manusia (Naor dan Shamir, 1995). Berbagai penelitian tentang kriptografi visual telah dilakukan, diantaranya Park et al. memperkenalkan sebuah metode kriptografi visual dengan menggunakan *codebook*. Namun, *shares* yang dihasilkan terlihat seperti titik-titik acak, sehingga dapat menimbulkan masalah manajemen *sharing* karena semua *shares* terlihat sama dan dapat menimbulkan resiko kecurigaan pihak ketiga dalam proses transmisi (Park et al., 2008). Pada tahun 2009, Wang et al. memperkenalkan sebuah metode kriptografi visual skema (k, n) dengan menggunakan gambar kamuflase (gambar tersamar) yang berbeda untuk mengidentifikasi *shares* sehingga dapat meningkatkan kemudahan manajemen. Namun, metode ini memiliki kelemahan yaitu ekspansi piksel yang besar sehingga hasil *share* mengalami perbesaran dari *secret image* dan kualitas rekonstruksi yang buruk (Wang et al., 2009). Pada tahun 2013, Liu et al. memperkenalkan sebuah skema kriptografi visual untuk citra warna yaitu skema $((n-1,1),n)$, dimana $(n-1)$ *natural image* digunakan sebagai *input* untuk menghasilkan *n* buah *shares*. Hasil pengujian yang dilakukan oleh Liu et al. menunjukkan bahwa enkripsi menggunakan skema ini dapat mengatasi masalah ekspansi piksel dan rekonstruksi *share* dapat dilakukan tanpa distorsi (Liu et al., 2013). Namun, *share* yang dihasilkan akan menarik perhatian pihak lain dan menimbulkan kecurigaan karena sifatnya acak.

Untuk mengurangi kecurigaan pihak lain terhadap *share,* maka dilakukan teknik pengamanan lain yaitu steganografi, dimana *share* akan disembunyikan ke dalam gambar (Li et al., 2014). Muhammad et al. memperkenalkan metode steganografi menggunakan citra warna. Pada metode ini *secret image* disisipkan

pada *Least Significant Bit* dari *cover image* secara *random* dan siklis, dimana bit *secret image* akan disisipkan pada nilai *Red, Green, Blue, Red, Green, Blue* dan seterusnya hingga semua bit *secret image* selesai disisip. Akan tetapi metode ini memiliki PSNR yang rendah (Muhammad et al., 2014). Kemudian pada tahun 2015, Muhammad et al. memperkenalkan teknik steganografi dengan menggunakan warna Hue-Saturation-Intensity berbasis LSB. Kelebihan dari model warna ini adalah sesuai untuk menggambarkan warna berdasarkan interpretasi manusia dan komponen Intensitas tidak berkorelasi dengan komponen Hue dan Saturasi (Plantaniotis dan Venetsanopoulos, 2000). Disamping itu, model warna HSI dapat menyembunyikan data yang lebih besar dan proses ekstraksi yang lebih rumit dibandingkan dengan model warna lain (RGB dan CMYK) (Kaur dan Deep, 2015). Proses penyembunyian dilakukan dengan mengkonversi warna RGB sebagai sampul menjadi warna HSI, kemudian menyisipkan pesan ke dalam nilai Intensitas menggunakan teknik LSB dan mengkonversi kembali ke dalam warna RGB. Hasil analisis oleh Muhammad et al., pengamanan data menggunakan model warna HSI menunjukkan data tidak dapat dikenali (*good imperceptibility*) (Muhammad et al., 2015). Namun, metode ini masih memiliki kelemahan, yaitu proses ekstraksi dapat dilakukan oleh siapa saja yang mengetahui jumlah bit sisip dengan melakukan konversi dari RGB ke HSI. Oleh karena itu dibutuhkan pengamanan lainnya yaitu dengan penambahan *password* berupa karakter pada *stego image*.

Berdasarkan uraian di atas, maka penerapan kriptografi visual dan model warna HSI diangkat sebagai tugas akhir dengan judul **"Penerapan Model Warna HSI Dan *Password* Pada Kriptografi Visual Skema $((n-1,1),n)$ Untuk Meningkatkan Keamanan Citra Berwarna".**

1.2. Rumusan Masalah

Berdasarkan uraian pada latar belakang di atas, maka yang menjadi permasalahan sehingga perlu dilakukan penelitian ini adalah:

1. *Share* yang dihasilkan pada skema $((n-1,1),n)$ kriptografi visual dapat menimbulkan kecurigaan pihak lain.

2. Pengamanan citra menggunakan skema $((n-1,1),n)$ kriptografi visual dan model warna HSI tidaklah cukup, karena siapa saja bisa mengambil bit *share* dan mendapatkan *secret image* dengan melakukan konversi dan rekonstruksi.

1.3. Ruang Lingkup

Ruang lingkup dalam tugas akhir ini, adalah:

1. *Secret image* dan *natural image* yang dapat di-*input* merupakan citra RGB dengan format .jpg/ .jpeg, .png dan .bmp.
2. Jumlah *n* yang harus di-*input* adalah minimal 3 dan maksimal 10 dimana, $(n-1)$ merupakan jumlah *natural image* yang harus di-i*nput.*
3. *Cover image* memiliki ukuran minimal (*width* dan *height*) $\left\lfloor\sqrt{\frac{x}{b}}\right\rfloor$, dimana *x* merupakan jumlah bit panjang *password* + jumlah bit panjang *share* + jumlah bit *password* + jumlah bit *share,* sedangkan *b* merupakan jumlah bit nilai Intensitas yang akan digantikan dengan bit *share* $(1 \leq b \leq 4)$.
4. Panjang *password* yang digunakan minimal 6 karakter dan maksimal 14 karakter yang terdiri dari kombinasi angka, huruf kapital, huruf non-kapital dan karakter khusus.

1.4. Tujuan

Tujuan dari tugas akhir ini adalah membangun perangkat lunak dengan menerapkan model warna HSI dan skema $((n-1,1),n)$ kriptografi visual untuk pengamanan citra warna sehingga dapat mengurangi kecurigaan pihak lain terhadap *secret image* dan meningkatkan keamanan *secret image* dengan adanya penambahan *password.*

1.5. Manfaat

Manfaat yang diharapkan dari tugas akhir ini, adalah:

1. Perangkat lunak dapat digunakan sebagai alternatif pengamanan citra warna.
2. Perangkat lunak dapat dijadikan sebagai *library* untuk pengembangan sistem kriptografi visual yang lebih besar.

1.6. Metodologi Penelitian

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

1. Mempelajari referensi

   Pada tahap ini mempelajari referensi yang ada, dengan tujuan untuk memahami proses kerja dari metode yang digunakan pada tugas akhir.
2. Membuat aplikasi dengan model *waterfall*
   a. Analisis kebutuhan

      Pada tahap ini dilakukan analisis kebutuhan, berupa kebutuhan fungsional, non-fungsional dan analisis proses. Untuk kebutuhan fungsional terdiri dari:

      i. Embedding.
      ii. Ekstrak.

   b. Perancangan

      Pada tahap ini dilakukan perancangan *user interface* dari aplikasi, seperti Pembentukan Share (a), Pembentukan Share (b), Penyisipan Bit Share, Ekstrak Share, Rekonstruksi Share dan lain-lain.

   c. Penulisan program

      Pada tahap ini dilakukan penulisan kode program berbasis dekstop menggunakan *Visual C#.Net*.

   d. Pengujian

      Adapun pengujian yang akan dilakukan pada tahap ini adalah sebagai berikut:

      i. Melakukan pengujian terhadap pengaruh nilai bit sisip (*b)* dan kontras *cover* yang berbeda terhadap hasil *stego*, dimana *b* merupakan jumlah bit Intensitas citra HSI yang akan digantikan dengan bit *share* dan bit *password*.

ii. Melakukan pengujian terhadap *stego image* yang diberi *noise* terhadap kualitas citra hasil rekonstruksi. Jenis *noise* yang dapat diberikan yaitu *noise* Uniform yaitu *noise* dengan penyebaran seragam, *noise* Gausian dimana efek dari *noise* ini adalah munculnya titik-titik berwarna yang jumlahnya sama dengan presentase *noise*, *noise* Salt pepper yaitu *noise* yang seperti halnya taburan garam yang akan memberikan warna putih pada titik yang terkena *noise* dan *noise* Speckle yaitu model *noise* yang memberikan warna pada titik yang terkena *noise*.

3. Menarik kesimpulan dari hasil pengujian