BAB I
PENDAHULUAN

1.1 Latar Belakang

Visual secret sharing scheme (VSSS) merupakan suatu metode untuk mendistribusikan citra rahasia (*secret*) kepada setiap *n* peserta yang berkesuaian akan menerima suatu bagian (*share*) dimana untuk proses rekonstruksi dapat dilakukan dengan minimal *t share* dari jumlah *n* peserta (Moni Naor dan Adi Shamir., 1995). VSSS yang diperkenalkan Naor dan Shamir terbatas hanya untuk data berupa biner. Pada tahun 2002, Thien dan Lin memperkenalkan skema *secret image sharing* berdasarkan (*t,n*) dimana *secret image sharing* terbagi atas dua skema yaitu *linear* dan *nonlinear*. Dalam skema *linear,* setiap *n* peserta yang berhak dapat membangkitkan dan merekonstruksi rahasia dengan minimal *t share* yang menggunakan persamaan linier (Nandakumar et al, 2011). Kelemahan skema *linear* adalah rentan terhadap serangan *Tompa-Woll* yaitu berupa masalah kecurangan, dimana satu orang dalam kelompok dapat menipu jika citra rahasia terungkap secara tidak serentak (*asynchronous*) (Kurosawa et al, 2012).

Pada tahun 2014, Shin et al mengusulkan suatu skema *nonlinear secret sharing* berdasarkan (*t,n*) untuk berbagi citra rahasia. *Nonlinear secret sharing* akan membagi *secret image* (SI) menjadi beberapa *n shadow image* (SHI), kemudian SI tersebut tidak dapat direkonstruksi tanpa minimal *t share* dari citra yang telah di *share*. Dalam prosedur pembentukan *share*, terdapat sebuah variabel baru *m,* dimana *m* adalah bilangan bulat positif yang dipilih secara acak untuk mencegah terjadinya *overflow* ketika piksel diatas 255 atau keadaan *underflow* ketika piksel kurang dari 0. Hal ini dapat menyebabkan proses pembentukan dan penyisipan *share* tidak dapat dilakukan. Kemudian dikarenakan *share* yang berbentuk *shadow* tersebut dapat menimbulkan kecurigaan dari pihak lain, maka akan dilakukan teknik *embedding* dengan konsep steganografi modifikasi LSB. Steganografi menggunakan metode LSB (*Least Significant Bit*) yaitu algoritma sederhana yang menukar bit paling kanan ke dalam

beberapa *bit* dari *channel* yang telah di tentukan untuk menghasilkan *stego image*. Modifikasi LSB (*LSB Modification*) yang akan dilakukan adalah teknik *embedding* berdasarkan bilangan prima *p*, dengan adanya teknik tersebut *stego image* yang tersembunyi tidak akan hancur jika penyusup mengubah LSB dari semua piksel citra (Shin et al, 2014).

Untuk memperkuat pengamanan citra yang akan di distribusikan, maka digunakan sebuah teknik enkripsi. AES (*Advanced Encryption Standard*) merupakan algoritma standar dalam berbagai *platform* yang masih dianggap aman sampai saat ini (NIST, 2001). Kemudian untuk membuktikan kebenaran (*validity*) dari *share* yang dihasilkan, maka digunakan sebuah skema tanda tangan digital yang berguna untuk memastikan bahwa citra tersebut adalah yang sebenarnya. ECDSA (*Eliptic Curve Digital Signature Algorithm*) adalah salah satu skema tanda tangan yang menggunakan kurva eliptik (*elliptic curve*) atas suatu *prime finite field* sehingga lebih fleksibel dalam proses menentukan kunci. Tingkat keamanan ECDSA cukup tinggi dan memiliki panjang bit kunci yang relatif kecil (Kusuma et al, 2014).

Berdasarkan uraian di atas, maka topik ini diangkat sebagai tugas akhir dengan judul "***Nonlinear Image Secret Sharing* Citra Warna Dengan Tambahan Enkripsi, Tanda Tangan dan Modifikasi Lsb".**

1.2 Rumusan Masalah

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

1. Bagaimana pengaruh perubahan parameter *m* dan bilangan prima (GF(*p*)) terhadap kondisi *overflow* dan *underflow* terhadap proses pembentukan dan penyisipan *share.*
2. Bagaimana pengaruh parameter jumlah bit sisip dan mode sisip terhadap kualitas *stego images*.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah

1. Membangun aplikasi *nonlinear image secret sharing* citra warna dengan tambahan enkripsi, tanda tangan dan modifikasi LSB untuk menghindari terjadinya pencurian dan pemalsuan data gambar.
2. Mengetahui tingkat keamanan dari sistem yang dibangun dengan mengubah parameter *m* dan GF(*p*), bit sisip dan mode sisip terhadap kualitas *stego images*.

1.4 Manfaat

Manfaat yang diharapkan dari tugas akhir ini, adalah:

1. Sistem yang dibuat dapat digunakan sebagai alternatif pengamanan citra.
2. Hasil pengujian dapat digunakan untuk mengetahui pengaruh dari skema *nonlinear image secret sharing* citra warna dengan tambahan enkripsi, tanda tangan dan modifikasi LSB terhadap kelemahan serangan *Tompa* dan *Woll*.
3. Laporan Tugas Akhir dapat digunakan sebagai referensi untuk pengembangan sistem kriptografi menggunakan *nonlinear image secret sharing*.

1.5 Batasan Masalah

Batasan masalah dalam tugas akhir ini, antara lain:

1. Citra yang digunakan untuk menampung data adalah citra RGB 24 dengan format .bmp.
2. Citra yang akan diamankan merupakan citra persegi dengan ukuran minimal 50 x 50 pixel dan maksimal 200 x 200 pixel.
3. Algoritma enkripsi *Advanced Encryption Standard* (AES) yang digunakan adalah AES-256.
4. Dalam pembentukan tanda tangan digital parameter yang diperlukan adalah:
   a. Fungsi *hash* satu arah SHA-256 bit dan jumlah bit yang digunakan adalah 32 bit.

b. Kurva eliptik $y^2 = x^3 + ax + b\ (mod\ p)$ yang digunakan untuk algoritma ECDSA hanya menggunakan nilai a = 1 dan b = 1 maka $y^2 = x^3 + x + 1(mod\ p)$ dan bidang terbatas F_p

c. Bilangan prima yang digunakan untuk pembentukan kunci adalah $2 \leq p \leq 251$.

5. Dalam pembentukan *nonlinear secret sharing* parameter yang diperlukan:
   a. Bilangan positif *m* yang dipilih secara random dimana $m \leq p$ dan nilai bilangan prima *p* adalah $2 \leq p \leq 251$.
   b. Jumlah *n* yang harus di-*input* oleh *user* adalah minimal 5 dan maksimal 10.
   c. Jumlah *t* yang harus di-*input* oleh *user* minimal 2 dan maksimal sama dengan jumlah *n* yang ada.
6. Modifikasi LSB yang dilakukan adalah dengan teknik *embedding* LSB1 dan LSB2 dimana:
   a. bit sisip adalah 1 dan 2 bit
   b. *channel* warna RGB yang digunakan untuk menyisipkan *share* adalah *channel* RGB
7. Mode penyisipan yang digunakan adalah:
   a. *Sequencial Movement Scheme*
   b. *Snake Movement Scheme*
8. Untuk menentukan Amplop Khusus (menampung Parameter Masukan), maka ditetapkan aturan-aturan sebagai berikut:
   a. Ukuran amplop yang ditentukan adalah 200 x 200
   b. Parameter Masukan (PM) = Kunci AES 256 + Kunci kurva eliptik +*Message digest* + Tandatangan digital + t + n + m + jumlah bit sisip + mode sisip.

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. Analisis masalah

   Pada tahapan analisis masalah, dilakukan definisi rumusan masalah dan batasan masalah dalam sistem, kemudian dilakukan analisis terhadap masalah yang telah didefinisikan.

3. Membuat aplikasi dengan model *waterfall*

   a. Analisis kebutuhan

      Pada tahap ini dilakukan analisis kebutuhan sistem, berupa analisis proses, kebutuhan fungsional, dan kebutuhan *non*-fungsional. Untuk kebutuhan fungsional menggunakan *use case*, kebutuhan *non*-fungsional memanfaatkan PIECES dan *Flow Chart* untuk menganalisis proses.

   b. Perancangan

      Merancang langkah-langkah proses dengan *Flow Chart* dan merancang *user* interface dengan aplikasi *Visio* dan *Balsamiq*.

   c. Penulisan program

      Melakukan penulisan kode program menggunakan C#.net.

   d. Pengujian

      i. Melakukan pengujian pada pengaruh perubahan parameter *m* dan bilangan prima (GF(*p*)) terhadap kondisi *overflow* atau *underflow*. Pengujian tidak akan berhasil jika parameter *m* dan bilangan prima (GF(*p*)) pada proses pembentukan *share* tidak sesuai dengan ketentuan.

      ii. Melakukan pengujian *imperceptibility* pada pengaruh jumlah bit sisip dan mode sisip terhadap kualitas stego *images*. Agar pengujian terhadap citra lebih terukur, maka dilakukan perhitungan PSNR terhadap citra asli dan *stego image*. Jika nilai PSNR yang dihasilkan >= 40dB, maka *imperceptibility* tinggi.

e. Menarik kesimpulan dari hasil pengujian

   Penarikan kesimpulan diambil berdasarkan hasil pengujian yang dilakukan pada tahap sebelumnya.

f. Menyusun laporan Tugas Akhir berdasarkan referensi yang diperoleh dan hasil pengujian dari sistem hasil kontruksi.