BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan metode autentikasi dengan *username* dan *password* merupakan metode paling umum dan sederhana untuk sistem autentikasi. Namun, ketika dalam kondisi yang sebenarnya, banyak pengguna yang mengalami lupa *password*, sehingga fitur lupa *password* sering diakses oleh pengguna. Kasus yang kerap kali terjadi adalah terdapat pihak yang tidak bertanggung jawab dan mencoba untuk mendapat akses ke akun pengguna, untuk mengubah data, mencuri informasi rahasia, dan menyalahgunakan akun pengguna[1].

Penggunaan *password* secara konvensional untuk *login*, masih menjadi pilihan yang umum karena kemudahannya, walaupun banyak kelemahan yang sudah diketahui[2]. Salah satunya jenis serangan *brute-force* dimana peretas perlu memasukkan semua kemungkinan *password* yang digunakan pengguna. Contohnya peretas mencoba setiap kombinasi kata yang sederhana dan mudah diingat oleh pengguna yang berhubungan dengan tanggal lahir dan sebagainya. Selain *brute-force* ada juga bentuk ancaman lain dari sistem autentikasi konvensional yaitu *phishing*. *Phishing* mengarahkan pengguna untuk mengunjungi situs web palsu salah satunya dengan cara mengirimkan situs web tersebut melalui *email*, *SMS*, *Whatsap* dan lain-lain. Dengan cara ini, peretas dapat memperoleh informasi sensitif, seperti nama pengguna, *password*, kode PIN, informasi pribadi, dan kartu kredit[3].

Salah satu inovasi pengembangan sistem autentikasi adalah dengan menggunakan metode Steganografi. Steganografi merupakan kombinasi seni dan ilmu yang memungkinkan untuk menyisipkan pesan atau data melalui media digital seperti gambar, audio, dan video, guna meningkatkan keamanan sistem autentikasi[4].

Dari banyaknya inovasi dalam sistem autentikasi login yang diteliti, salah satunya adalah login menggunakan steganografi gambar seperti yang ditulis

pada jurnal yang berjudul ***"Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination",*** dijelaskan pada jurnal tersebut penggunaan autentikasi login dengan metode kombinasi AES dan LSB dapat berjalan dengan baik[5].

Salah satu keunggulan steganografi menggunakan LSB adalah proses perhitungan yang mudah untuk diimplementasikan. Cara kerja algoritma LSB dalam penyisipan pesan pada suatu media adalah dengan menyisipkan rangkaian bit pesan ke dalam bit terakhir dari setiap piksel dalam gambar. Proses kombinasi algoritma AES dan LSB adalah *password* dienkripsi terlebih dahulu menggunakan metode AES sebelum disisipkan ke dalam gambar menggunakan algoritma LSB. Hasilnya adalah *password* yang telah diubah ke dalam bentuk *ciphertext* sebelum diintegrasikan ke dalam citra. Kemudian *ciphertext* tersebut disisipkan ke dalam gambar yang digunakan untuk autentikasi *login*[6].

Keunggualan dari algoritma AES dibandingkan teknik enkripsi lainnya adalah AES mendukung enkripsi untuk data dalam jumlah besar dan lebih efisien dibanding dengan algoritma enkripsi lain[7]. Selain itu algoritma AES menjadi standar algoritma enkripsi baru yang diterbitkan oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001 sebagai pengganti algoritma DES, yang dianggap lebih tua dan lebih mudah diretas[8].

Namun metode *login* seperti ini bukan tanpa celah, salah satunya adalah data *ciphertext* yang akan dimasukkan kedalam gambar tentu saja akan memberikan dampak seperti membesarnya ukuran gambar. Salah satu algoritma yang dapat digunakan agar data yang disisipkan kedalam gambar tidak terlalu besar, adalah menggunakan algoritma kompresi. Diantara banyaknya algoritma untuk mengkompresi teks, salah satunya adalah algoritma Huffman. Algoritma ini merupakan algoritma kompresi *lossless* dimana data yang dikompresi dapat direkonstruksi ke dalam bentuk semula. Implementasi algoritma Huffman ini menggunakan Huffman *tree* yang menghitung frekuensi kemunculan data[9].

Dari beberapa keunggulan algoritma kompresi Huffman di atas, penelitian ini akan membahas tentang bagaimana menerapkan algoritma kompresi pada sistem autentikasi Steganografi menggunakan gambar. Maka dari itu diangkatlah penelitian ini dengan judul **"*Implementasi Algoritma Huffman Untuk Kompresi Ciphertext Advanced Encryption Standard 128 Pada Autentikasi Berbasis Penyisipan Gambar*"**.

1.2 Perumusan Masalah

Berdasarkan dari latar belakang yang telah dijelaskan di atas, maka dapat merumuskan masalah yaitu:

1. Bagaimana penerapan algoritma Huffman pada sistem autentikasi berbasis penyisipan gambar dengan *AES 128 dan LSB* ?
2. Bagaimana kinerja algoritma Huffman pada sistem autentikasi berbasis penyisipan gambar dengan *AES 128 dan LSB* ?

1.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Menerapkan algoritma Huffman pada sistem autentikasi berbasis penyisipan gambar dengan *AES 128 dan LSB*;
2. Mengetahui kinerja dari algoritma Huffman pada sistem autentikasi berbasis penyisipan gambar dengan *AES 128 dan LSB*.

1.4 Batasan Masalah

Batasan masalah yang terdapat pada penelitian ini yaitu :

1. Gambar yang bisa digunakan hanya gambar berformat .PNG;
2. *User* dapat *login* menggunakan gambar yang telah disisipkan data sebelumnya;
3. Pengelolaan gambar dan data yang dienkripsi dapat dilakukan di halaman utama setelah melakukan *login*;
4. Pengujian akan dilakukan dengan menggunakan 30 gambar;
5. Data yang dikompresi dengan Algoritma Huffman merupakan data *ciphertext*, bukan gambarnya;
6. Satu *user* bisa menambahkan gambar pada sistem ini maksimal 6 gambar;

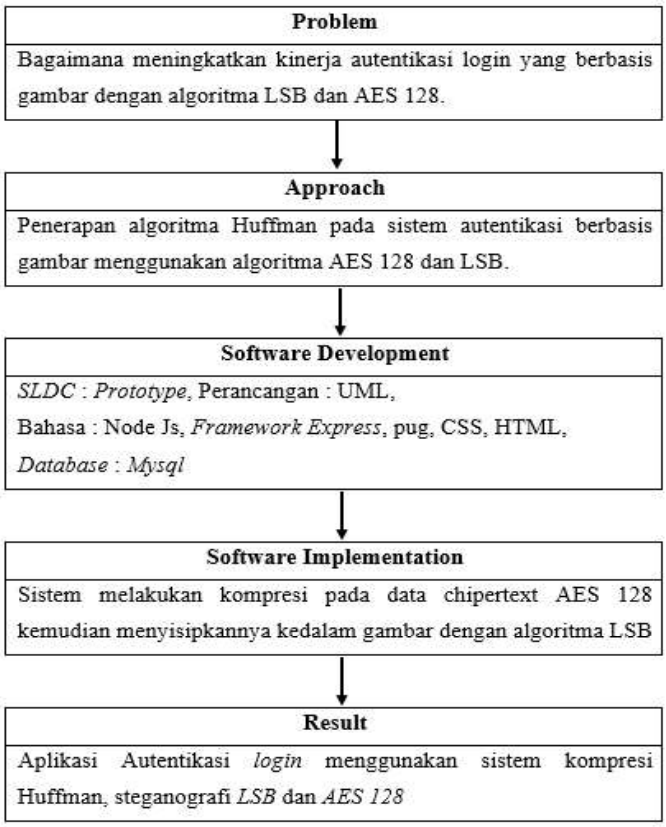
7. *Username* dan *password* yang dimasukkan oleh *user* harus berbeda.

1.5 Manfaat Penelitian

Manfaat pada penelitian ini adalah mengurangi jumlah karakter pada *ciphertext* yang akan dimasukan kedalam gambar, sehingga gambar memiliki ukuran yang lebih kecil dari sebelumnya, dan diharapkan mampu memberikan kinerja yang baik untuk sistem keamanan dengan *login* berbasis penyisipan gambar dimana gambar yang telah disisipi data kompresi memiliki ukuran yang lebih kecil dibandingkan gambar yang tanpa melalui proses kompresi sebelumnya.

1.6 Kerangka Pemikiran

Kerangka Pemikiran dari perancangan sistem ini terdapat pada gambar 1.1 Kerangka Pemikiran.



Gambar 1. 1 Kerangka Pemikiran

1.7 Metodologi Penelitian

1.7.1 Metodologi Penelitian

Pendekatan yang diterapkan dalam pengumpulan informasi melibatkan metode penelitian deskriptif yang bertujuan untuk menyajikan gambaran yang komprehensif dan netral mengenai permasalahan yang dibahas. Berikut ini merupakan metodologi yang digunakan untuk mengumpulkan data tersebut :

1. Observasi, merupakan kegiatan yang melibatkan pengawasan langsung terhadap objek penelitian di dalam domain penelitian guna memperoleh informasi yang diperlukan;
2. Studi Literatur, adalah proses menyelidiki informasi tertulis yang terkandung dalam karya sastra, penelitian ilmiah, dan laporan penelitian yang berhubungan dengan subjek penelitian yang sedang diselidiki.

1.7.2 Metodologi Pengembangan

Sistem ini dibangun dengan menggunakan pendekatan *prototype*, yang melibatkan serangkaian langkah eksperimen tanpa perlu menunggu penyelesaian sistem secara keseluruhan. Tahapan yang digunakan diantaranya:

1. *Requirement Gathering*

   Pada tahap ini, dilakukan analisis kebutuhan untuk membangun sistem, seperti identifikasi *hardware* dan *software* yang akan digunakan.
2. *Quick Design*

   Pada tahap ini dilakukan perancangan desain *user interface* yang nantinya akan digunakan.
3. *Building Prototype*

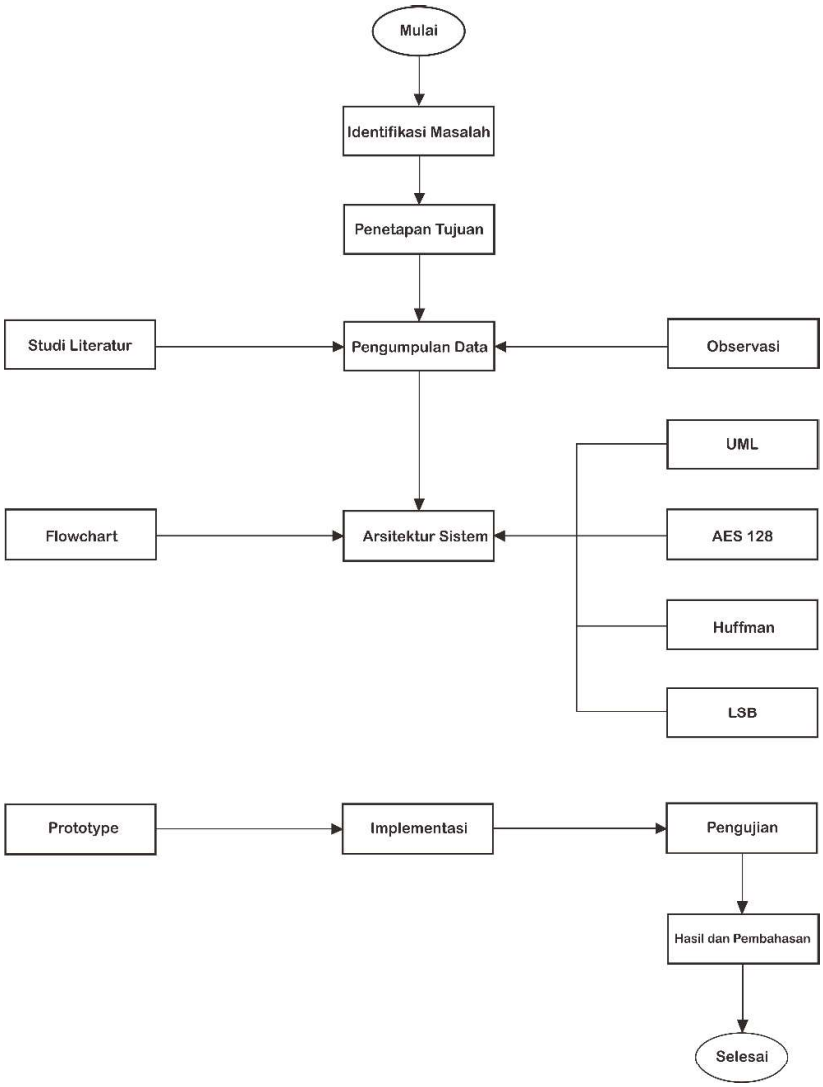
   Tahap ini adalah tahap pengerjaan perangkat lunak yang telah dirancang pada lalu semuanya diimplementasikan, tahapan yang terdapat pada tahapan ini contohnya ialah pembuatan kode program hingga selesai lalu diuji tingkat keberhasilannya.

4. *Evaluation of Prototype*

   Tahap ini adalah tahapan terakhir dimana terdapat evaluasi atau pengujian dari sistem perangkat lunak yang telah dibangun dan kemudian perbaikan *bug* yang masih ditemukan.

1.8 Alur Penelitian

Berikut merupakan Alur Penelitian yang digambarkan pada Gambar 1.2 Alur Penelitian.



Gambar 1. 2 Alur Penelitian

1.9 Sistematika Penulisan

Sistematika Penulisan adalah representasi keseluruhan yang terdapat dalam penyusunan karya riset ini beserta uraiannya :

BAB I PENDAHULUAN

Bab I meliputi informasi mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta tata cara penulisan yang terstruktur.

BAB II KAJIAN LITERATUR

Bab II menjelaskan tentang konsep-konsep teoritis yang relevan dengan penelitian ini, mulai dari proses hingga implementasi. Bagian ini juga mencakup penjelasan mengenai penelitian terdahulu yang berhubungan dengan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab III mencakup evaluasi dan perencanaan perangkat lunak yang dibuat berdasarkan isu-isu yang telah diidentifikasi dalam Bab II.

BAB IV HASIL DAN PEMBAHASAN

Bab IV menjelaskan penerapan sistem yang meliputi aspek-aspek seperti perangkat keras, basis data, antarmuka, serta pengujian sistem melalui metode *blackbox testing* dan ringkasan pengujian yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Bab V berisi kesimpulan dan saran mengenai hasil penelitian yang telah dilakukan, serta saran untuk perkembangan penelitian mendatang.