BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam Pemilihan Umum (Pemilu) pada tahun 2019, pasangan calon nomor urut 02 Prabowo-Sandi melakukan tudingan kecurangan-kecurangan yang dilakukan oleh pasangan calon nomor urut 01 Jokowi-Maaruf, beberapa bentuk kecurangan itu dilakukan oleh Badan Pemenangan Nasional (BPN) pada hasil pemungutan suara yang dilakukan secara serentak seluruh provinsi Indonesia. Dugaan bentuk kecurangan yang dilakukan oleh pasangan calon nomor urut 01 adalah merubah hasil suara dan telah dilakukan pencoblosan pada lembar pemilihan suara sebelum dikirim ke tempat TPS daerah-daerah seluruh provinsi Indonesia.

Sebagai contoh dugaan kesalahan *input* yang dilakukan oleh Komisi Pemilihan Umum (KPU) yaitu di TPS 30, Bojongsari, Depok, Jawa Barat. Suara pasangan nomor urut 02 berubah dari 148 menjadi 3, sementara pasangan calon nomor urut 01 bertambah dari 63 suara menjadi 211 suara. KPU telah memberikan penjelasan. Menurutnya, kesalahan dalam input data C1 ke SITUNG *Real Count* pemilihan Presiden 2019 bisa datang dari berbagai kemungkinan. Selain factor *human error* kesalahan juga bisa datang dari faktor kesengajaan (News T. , Temuan Kesalahan Input Data Penghitungan Suara, Ketua KPU: Tidak Ada Niat Curang, 2019).

KPU RI menjelaskan Sistem Informasi Penghitungan (Situng) selain mempuyai fungsi transparansi informasi hasil pemilu, juga bermanfaat untuk rujukan bila ditemukan dokumen formulir C1 yang janggal. KPU RI menyatakan demikian untuk menanggapi peristiwa penyitaan dua kardus berisi ribuan formulir C1 yang diangkut dengan sebuah mobil, untuk membedakan formulir C1 asli atau palsu bisa dengan pembuktian dengan cara menyandingkan antara scan formulir C1 yang ada di situng, dengan formulir C1 yang palsu (News T. , 2019).

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Disebabkan pesatnya perkembangan

ilmu pengetahuan dan teknologi yang memungkinkan munculnya teknik-teknik baru, yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, di mana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan.Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Data dapat berupa sebuah file dan berbentuk string (Hasugian, 2017).

Kita telah banyak melihat dan mendengar kajadian pada dunia komputer, khususnya jaringan internet, yang menghadapi serangan virus, *worm, Trojan, DoS, deface,* pembajakan software, masalah pencurian kartu kredit sampai memanipulasi identitas orang lain. Ada beberapa yang bisa terserangnya sistem keamanan pada jaringan komputer ialah;

- *Rilis Security Patch* yang sering terlambat. Seringkali administrator terlambat melakukan *patching* keamanan (instalasi program perbaikan yang berkaitan dengan kemanan suatu sistem) misalnya karena banyaknya komputer atau sever yang harus ditanganinya.
- Hukum dan kurangnya Sumber Daya Manusia. Kesulitan yang utama dari penegak hukum adalah mengejar kemajuan dunuia komputer dan telekomunikasi yang sangat cepat. Payung hukum harus dibuat untuk melindungi para pengguna di dunia *cyber* (Keraf A. Sonny, 2001).

Dengan harus diadakan keamanan lebih dari *software* itu sendiri maka dari penggunanya juga harus melakukan sebuah keamanan berupa text yang di Kriptografikan dan disisipkan kedalam gambar. Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman.

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (encrypted) dengan menggunakan sebuah kunci (key). Untuk membuka (decrypt) data tersebut digunakan juga sebuah kunci yang sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*). Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan gunsi enkripsi dan deskripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika (Sasongko, 2005).

Algoritma simetrik dapat pula disebut sebagai algoritma konvensional, dimana kunci dekripsi dapat ditentukan dari kunci enkripsinya, begitu pula sebaliknya. Pada algoritma simetrik, kunci enkripsi dan kunci dekripsinya sama. Keamanan dari algoritma ini terletak pada kuncinya, jika kunci diberitahukan atau dibocorkan maka siapa saja dapat mengenkrip dan mendekrip data, jadi kunci harus benar-benar rahasia dan aman (Dafid, 2006).

Pada blok *cipher*, *plaintext* yang akan disandikan dipecah menjadi blok-blok dengan panjang yang sama. Blok *cipher* menyandikan setiap *plaintext* tersebut menjadi blok *ciphertext* dengan proses enkripsi yang identik dan keseluruhan blok *plaintext* disandikan dengan kunci yang sama. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia (Dafid, 2006).

Steganografi adalah teknik penyembunyian data rahasia ke dalam sebuah media sehingga data yang disembunyikan sulit dikenali oleh indera penglihatan manusia. Steganografi membutuhkan dua properti yaitu media penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai media penampung, misal gambar, suara, teks dan video (Maradilla, 2012). Metode steganografi itu bisa dikatakan lebih aman karena sifatnya yang tidak mengacak, sehingga file yang disisipi tidak mencurigakan, walaupun setiap metode memiliki kelebihan dan kekurangan masing-masing dan metode ini cara efektif dalam menyembunyikan pesan rahasia dan telah digunakan selama berpuluh-puluh tahun (Nani, 2011).

Menurut Aditya, Pratama, Nurlifa (2010), metode yang dibandingkan yaitu metode *Least Significant Bit* (LSB) dan *End Of File* (EOF). Kedua metode ini memiliki kekurangan dan kelebihan masing-masing, LSB dan EOF ini merupakan metode yang sering digunakan untuk pengembangan steganografi citra. Penyembunyian data enkripsi yang disisipi di dalam citra dengan metode *End Of File* (EOF) lebih terjaga dari kualitas gambar namun disisi ukuran file akan lebih besar sesuai data enkripsi yang disisipi dan untuk metode *Least Significant Bit* (LSB) ukuran file tetap terjaga namun kualitas citra agak mengurangi dari citra semula yang sebelum disisipi data enkripsi (Aditya, Pratama, & Nurlifa, 2010).

Menurut Nani (2011), dalam penelitiannya memadukan kelebihan algoritma Blowfish (kriptografi) dan metode *End Of File* (EOF) dimana "pesan rahasia" dienkripsi terlebih dahulu menggunakan algoritma Blowfish, lalu setelah itu disisipkan pada citra digital menggunakan metode EOF. Untuk melakukan metode EOF merupakan teknik yang relatif mudah dimengerti dan melakukan enkripsi pesan yang ingin disisipkan keamanan pasti akan terjaga, namun pada penelitiannya ini menyebutkan bahwa ada kelemahan pada steganografi sendiri yaitu dapat dengan mudah diekstrak oleh orang-orang yang tidak bertanggungjawab menggunakan software steganalysis yang beredar luas di dunia maya (Nani, 2011). Oleh karena itu, untuk mengatasi kekurangan dari metode steganografi tersebut maka dalam penelitian ini akan memodifikasi penempatan bit-bit pesan rahasia yang disisipi pada citra.

Metode yang paling sederhana adalah metode modifikasi *Least Significant Bit* (LSB). Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB) (Munir, 2004). *Least Significant Bit* (LSB) merupakan salah satu teknik dalam Steganografi. LSB menambahkan bit data yang akan disembunyikan (pesan) di bit terakhir yang paling cocok atau kurang (Aditya et al., 2010).

Menurut Andrian (2013), dalam penelitiannya bahwa metode steganografi *Least Significant Bit* (LSB), penyusup yang dapat mengubah LSB dari semua piksel gambar. Dengan cara ini pesan tersembunyi akan dihancurkan dengan mengubah sedikit kualitas gambar yaitu di kisaran 1 atau -1 pada setiap posisi piksel. Untuk

mengatasi kelemahan ini, maka diperlukan pengembangan atau modifikasi dari metode LSB.

Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti.

Misalkan bit pada image dengan ukuran 3 pixel sebagai berikut (Munir, 2004):

0011111 | 11101001 | 11001000

0011111 | 11001000 | 11101001

1100000 | 00100111 | 11101001

Pesan yang akan disisipkan adalah karakter ‘A’ yang memiliki biner 10000001, stego image yang akan dihasilkan adalah :

0011111**1** | 1110100**0** | 1100100**0**

0011110 | 1100100**0** | 1110100**0**

1100000 | 0010011**1** | 11101001

1.2 Rumusan Masalah

Sesuai latar belakang masalah yang telah diuraikan pada sub bab sebelumnya, maka munculah rumusan masalah sebagai berikut:

1. Bagaimana cara membuat aplikasi keamanan data hasil suara dalam formulir C1 yang telah dienkripsi dengan mode ECB dan algoritma elgamal ke dalam citra formulir C1 dengan teknik steganografi LSB modifikasi?
2. Bagaimana cara memodifikasi penempatan pada bit-bit terakhir pada citra formulir C1 dengan steganografi LSB modifikasi?
3. Bagaimana hasil eksperimen mengenai keamanan data hasil suara menggunakan enkripsi mode ECB dan algoritma elgamal dengan teknik steganografi LSB Modifikasi?

1.3 Tujuan Penelitian

Setelah diketahui rumusan masalahnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Implementasi data hasil suara formulir C1 pada sebuah aplikasi dengan cara mode ECB dan algoritma elgamal dengan teknik steganografi LSB modifikasi penempatan bit pada citra.
2. Membuktikan cara steganografi citra formulir C1 dengan teknik LSB modifikasi.
3. Menganalisa keamanan data hasil suara pada formulir C1 yang telah di ubah ke *ciphertext* dengan mode ECB dan algoritma elgamal dalam citra formulir C1 steganografi LSB modifikasi.

1.4 Manfaat Penelitian

Adapun manfaat dalam penelitian ini, diantaranya sebagai berikut:

1. Memperkuat keamanan data hasil suara untuk penyisipan yang disisipkan pada bit-bit citra.
2. Mengurangi kriptanalis untuk meretas atau memanipulasi data hasil suara pada steganografi citra formulir C1 LSB modifikasi dalam citra.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini, diantaranya sebagai berikut:

1. Sistem Steganografi dikembangkan hanya untuk menyisipkan karakter huruf.
2. Dalam enkripsi plaintext hanya dengan mode ECB dan algoritma elgamal dengan melakukan penyisipan pesan teknik steganografi LSB modifikasi untuk menyamarkan pesan rahasia.

1.6 Sistematika Penulisan

Pada bagian sistematika penulisan ini akan diuraikan mengenai penjelasa tiap bab.

BAB I PENDAHULUAN

Bab ini menjelaskan bagaimana penelitian ini bisa muncul dan isinya mengenai konteks penelitian yang dilakukan, diawali dengan latar belakang masalah, rumusan masalah, tujuan penelitian manfaat penelitian, batasan masalah, dan sistematika penulisan.

BAB II KAJIAN PUSTAKA

Bab ini menjelaskan teori pendamping atau pendukung untuk melakukan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan langkah-langkah penelitian yang akan dilakukan, dimulai dari desain penelitian, bahan dan alat yang digunakan untuk penelitian dan yang terakhir teknik analisis untuk penelitian.

BAB IV HASIL & PEMBAHASAN

Bab ini menjelaskan hasil penelitian dan spesifikasi metode penelitian dari penulis yang telah di buat. Semua pertanyaan mengenai masalah yang diangkat dalam tema skripsi dibahas di sini.

BAB V KESIMPULAN

Bab ini menjelaskan penarikan kesimpulan dalam penelitian yang telah penulis rancang dan menjelaskan kekurangan, kelebihan, saran untuk peneliti selanjutnya.