BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Identitas pribadi merupakan data yang sensitif, jika data ini tidak disimpan dengan aman dan jatuh ke tangan yang salah, maka dapat menyebabkan kerugian yang serius (Majoras, dkk., 2005). Identitas pribadi yang biasa diincar sebagai target kejahatan adalah nama, alamat, *social security number (SSN)*, dan kata sandi (ITS, 2017).

Jones (2017) mengatakan melalui theguardian.com bahwa pada enam bulan pertama tahun 2017, sudah terjadi 89.000 kasus pencurian identitas. Dilansir dari techworld.com (2017), pada tahun 2017 sendiri, terungkap setidaknya delapan kasus *hacking* terhadap perusahaan besar seperti Delloite, Equifax, CEX, BUPA, Zomato, Wonga, Three, Sports Direct, dan masih banyak kasus lain yang terungkap sebelum tahun 2017. Kerugian yang diakibatkan oleh kejadian ini adalah tercurinya jutaan identitas pribadi seperti nama, alamat, tanggal lahir, *email*, nomor kartu kredit, dan *social security number* milik pelanggan.

Pada era sekarang ini, pencurian identitas menjadi suatu masalah keamanan yang serius. Dampak yang diakibatkan dari kejahatan ini dapat berupa kerugian materiil berupa finansial maupun bukan materiil. Korban dapat kehilangan reputasi dan posisi di masyarakat, bahkan dapat ditangkap untuk tindak kejahatan yang dilakukan pelaku pencurian identitas. Dampak tersebut tidak hanya dapat dirasakan oleh individu, tetapi dapat meluas hingga ke pemerintahan, bisnis, dan masyarakat umum. Pada dasarnya, pencurian identitas terjadi ketika identitas seseorang

disalahgunakan untuk mendapatkan suatu keuntungan tertentu yang biasanya berupa keuntungan finansial. Pelaku dari pencurian identitas ini dapat memanfaatkan identitas korban untuk melakukan transaksi finansial, membuka rekening bank, melakukan tindak kriminal, mengirim *email* ancaman, terorisme, bahkan memulai kehidupan yang baru menggunakan identitas korban (CIPPIC, 2017).

Pengamanan data sensitif seperti identitas dari tindak kejahatan, memerlukan suatu metode untuk mengamankan data tersebut, salah satu caranya menggunakan kriptografi (Marisman & Hidayati, 2015). Kriptografi adalah ilmu yang bertujuan untuk membuat informasi yang sensitif menjadi tidak dapat dibaca kecuali oleh orang yang berhak (Desoky, 2005). Pada penelitian berjudul "Pengamanan Data dengan Menggunakan Algoritma Kriptografi AES, RC4 dan Kompresi LZ77 Berbasis Java pada Badan Karantina Pertanian" dijelaskan bahwa algoritma kriptografi bermanfaat untuk melindungi data penting dari pihak yang tidak bertanggung jawab (Siswanto, dkk., 2016).

Salah satu kriptografi yang bisa digunakan untuk mengamankan data yaitu kriptografi kurva eliptik. Kriptografi kurva eliptik merupakan kriptografi yang menggunakan kurva eliptik pada Matematika sebagai dasar keamanannya. Keuntungan kriptografi kurva eliptik dibandingkan dengan kriptografi lain yaitu memiliki tingkat keamanan yang sama namun dengan panjang kunci yang lebih pendek (Sembiring, 2015). Ukuran kunci yang kecil akan meningkatkan komputasi yang semakin cepat, konsumsi *power* yang rendah, dan menekan penggunaan *memory* dan *bandwidth* (Weku, 2012).

Hasil pengamanan data menggunakan kriptografi akan menimbulkan kecurigaan, sedangkan steganografi akan menyembunyikan keberadaan dari data tersebut agar tidak diketahui keberadaannya oleh pihak lain (Ahmed & Khalifa, 2014). Salah satu metode yang dapat digunakan dalam steganografi adalah Least Significant Bit (LSB). Least Significant Bit merupakan metode yang mengganti *bit* terkecil dari suatu media dengan *bit* dari pesan yang ingin disembunyikan. Perubahan yang diakibatkan metode ini pada suatu citra digital tidak akan menunjukkan perubahan yang berarti, sehingga tidak disadari oleh mata manusia (Wijaya, dkk., 2012).

Citra digital yang digunakan dalam penelitian ini adalah gambar dengan format Portable Network Graphic (PNG). Format PNG dipilih karena mampu menyortir lebih banyak transparansi dalam *colour depth* dibandingkan dengan format Graphics Interchange Format (GIF). PNG juga mendukung *grayscale, true color,* dan *indexed colours* (Alqahtani, dkk., 2016). Sedangkan untuk format lain seperti *Joint Photographic Experts Group* (JPEG), format ini belum mendukung kompresi *lossless*, sehingga saat dilakukan manipulasi, gambar akan kehilangan integritasnya (Sinha, 2015).

Berdasarkan latar belakang permasalahan yang telah dijelaskan, maka penelitian ini dibuat untuk mengimplementasikan kriptografi kurva eliptik dan steganografi Least Significant Bit untuk mengamankan identitas diri.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka masalah yang dirumuskan adalah bagaimana mengimplementasikan kriptografi kurva eliptik dan steganografi Least Significant Bit untuk penyimpanan identitas?

1.3 Batasan Masalah

Dari peneilitian yang akan dilakukan maka batasan masalah yang didefinisikan adalah sebagai berikut.

a. Data yang dienkripsi berupa teks.
b. Citra digital yang digunakan berupa gambar berformat PNG.
c. Gambar PNG yang digunakan memiliki minimal *size* berdasarkan ukuran *cipher text.*
d. Metode LSB menggunakan teknik 1-*bit insertion.*
e. Data diri yang akan disimpan adalah data diri pada Kartu Tanda Penduduk (KTP) Indonesia.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, maka tujuan dari penelitian ini adalah mengimplementasikan kriptografi kurva eliptik dan steganografi Least Significant Bit untuk penyimpanan identitas.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut.

a. Mengamankan penyimpanan data yang bersifat sensitif.
b. Menjadi referensi dalam pengembangan keamanan komputer terutama bidang kriptografi kurva eliptik dan steganografi *Least Significant Bit*.

1.6 Sistematika Penulisan Laporan Penelitian

Sistematika penulisan yang digunakan dalam penulisan laporan penelitian ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori yang digunakan sebagai landasan dalam melakukan penelitian yaitu pencurian identitas, kriptografi, steganografi, kriptografi kurva eliptik, *least significant bit*, dan *portable network graphics*.

BAB III METODOLOGI DAN PERANCANGAN APLIKASI

Bab ini berisi tentang tahapan dan rancangan aplikasi yang dilakukan dalam melakukan penelitian berupa metodologi penelitian yang dilakukan, *flowchart* aplikasi, dan rancangan tampilan antarmuka.

BAB IV IMPLEMENTASI DAN UJI COBA

Bab ini berisi tentang hasil implementasi algoritma sesuai dengan rancangan serta pembahasannya dalam menjawab rumusan masalah.

BAB V SIMPULAN DAN SARAN

Bab ini berisi tentang simpulan dari pembahasan dan saran bagi pembaca.