

BAB I PENDAHULUAN

1.1 Latar Belakang

Pada era digital ini penyebaran data digital sangat pesat, mengingat perkembangan internet dan dunia teknologi informasi yang terus maju secara keseluruhan. Ada beberapa faktor yang membuat data digital (seperti teks, citra, audio dan video) banyak digunakan antara lain karena data tersebut mudah diduplikasi dan hasilnya sama dengan aslinya, murah untuk penduplikasian dan penyimpanan, mudah disimpan untuk kemudian diproses lebih lanjut, serta mudah didistribusikan baik dengan media disk maupun melalui jaringan seperti internet. Apalagi dengan perkembangan internet yang dapat menyajikan dan mempersatukan berbagai jenis data digital, sehingga data digital tersebut semakin banyak digunakan untuk membentuk suatu sistem multimedia.

Pengiriman data multimedia secara online menghadapi masalah yang cukup besar dengan tidak adanya *framework* yang aman untuk melindungi data penting. Sedangkan pengiriman melalui CD atau *removable disk* menghadapi masalah besar karena pembajakan yang nyaris sempurna dari segi kualitas dan manipulasi data pada penggunaannya.

Salah satu karya intelektual yang dilindungi adalah barang dalam bentuk digital, seperti *software* dan produk multimedia seperti teks, musik atau citra (*image*) dan video digital. Selama ini penggandaan atas produk digital tersebut dilakukan secara bebas dan leluasa dengan hasil yang sama persis. Pemegang hak cipta atas produk digital tersebut tentu dirugikan karena tidak mendapat royalti dari usaha penggandaan itu.

Sebenarnya masalah penyalahgunaan hak cipta pada bidang multimedia tidak hanya mengenai penggandaan dan pendistribusian saja, tetapi juga mengenai label kepemilikan. Saat ini produk multimedia tersebut tidak hanya dapat didistribusikan secara offline, tetapi juga dapat dilakukan secara online melalui internet. Dan sebagian besar produk multimedia yang beredar di internet tidak

mencantumkan informasi pemiliknya, sehingga produk multimedia itu dapat diklaim oleh siapa saja sebagai hak miliknya.

Salah satu cara melindungi hak cipta multimedia adalah dengan menyisipkan informasi ke dalam data multimedia yaitu dengan cara *Watermarking*. Informasi yang disisipkan ke dalam data multimedia disebut *watermark*. Dan dapat dianggap sebagai sidik digital (*digital signature*) dari pemilik yang sah atas produk multimedia tersebut. Dengan kata lain, *watermark* yang disisipkan menjadi label hak cipta dari pemiliknya. Penyisipan data dengan *watermark* dilakukan sedemikian rupa sehingga informasi yang disisipkan tidak merusak data yang dilindungi. Data yang disisipkan bersifat tersembunyi dan keberadaannya tidak disadari oleh indra manusia. Jadi untuk membuktikan kepemilikan suatu produk multimedia, pemegang hak cipta dapat mengekstraksi tanda *watermark* yang telah disisipi ke data digital kemudian dilakukan dekripsi sampai sesuai dengan hasilnya, maka kepemilikan atas produk tersebut telah terbukti. Atas dasar inilah peneliti membuat Tugas Akhir dengan judul “IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI PUBLIK RSA DENGAN ALGORITMA STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB) SEBAGAI WATERMARKING UNTUK PELABELAN IDENTITAS PADA FILE CITRA DIGITAL”.

1.2 Rumusan Masalah

1. Berapa nilai *Mean Square Error* citra asli dengan citra hasil penyisipan menggunakan kombinasi metode RSA dan *Least Significant Bit*?
2. Berapa nilai *Peak Signal to Noise Ratio* dari perbandingan kualitas citra asli sebelum dan sesudah penyisipan label?
3. Berapa nilai akurasi ketepatan sistem dalam melakukan *dekripsi ciphertext* menjadi *plaintext*?

1.3 Batasan Masalah

Dalam penyusunan tugas akhir ini, diberikan batasan masalah agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan. Batasan masalah tersebut antara lain:

1. Bentuk implementasi berbasis *desktop* yaitu menggunakan *matlab*.
2. Jenis file yang digunakan sebagai media penyimpanan label berupa *file* gambar berwarna atau RGB 24 bit dengan *extension* .png.
3. Pesan yang disembunyikan adalah pesan teks dengan *extension* .txt.
4. Algoritma *kriptografi* yang digunakan adalah algoritma jenis *asimetris* dengan metode Kunci Publik RSA untuk *enkripsi* (*encryption*) dan *dekripsi* (*decryption*).
5. Algoritma *steganografi* untuk penyisipan (*embedding*) dan ekstraksi (*extracting*) menggunakan metode *Least Significant Bit*.
6. Skenario pengujian menggunakan 15 *file* gambar dengan kategori ukuran sebagai berikut:

Kecil	9,67kb - 12,5kb - 12,6kb - 13,8kb - 17,1kb
Sedang	105kb - 192kb - 375kb - 492kb - 984kb
Besar	1,725kb - 2,945kb - 23,398kb - 29,833kb - 32,535kb

 Pengujian dilakukan dengan menyisipkan pesan sebanyak 10 karakter, 100 karakter hingga 1000 karakter pada setiap *file* gambar.
7. *Output* yang didapat yaitu sebuah *file* yang telah melalui proses enkripsi dan penyisipan label.

1.4 Tujuan Penelitian

Tujuan penulisan tugas akhir rumusan masalah di atas adalah untuk mengetahui nilai *Mean Square Error* dari kombinasi metode RSA dengan *Least Significant Bit* serta membandingkan kualitas citra digital hasil penyisipan kombinasi RSA dan *Least Significant Bit* hingga berapa akurasi ketepatan sistem dalam melakukan *dekripsi ciphertext* menjadi *plaintext*.

1.5 Manfaat Penelitian

1. Dengan menggunakan metode yang sudah ada, diharapkan muncul gagasan baru dalam hal penyisipan data untuk peningkatan keamanan berbagai media.
2. Untuk dunia akademik sebagai acuan dalam teknik *kriptografi* dan *steganografi*.
3. Menambah wawasan atau pengetahuan alternatif untuk masyarakat cara memberi *watermarking* pada citra digital untuk hasil karyanya sendiri.