BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi di bidang telekomunikasi meningkat secara pesat. Komunikasi jarak jauh dilakukan untuk mengefisiensikan waktu dan tenaga agar kegiatan dapat dilakukan secara efektif. Selain itu, kondisi lain seperti pandemi yang mengharuskan setiap orang untuk menjaga jarak mengakibatkan tidak adanya pilihan lain bagi mereka untuk menggunakan perangkat telekomunikasi agar tetap dapat berkomunikasi satu sama lain. Teknologi telekomunikasi memudahkan setiap orang untuk berbagi data atau informasi. Akan tetapi, kemudahan ini juga dapat membahayakan tingkat keamanan dan kerahasiaan suatu data atau informasi karena data atau informasi tersebut dapat dengan mudah diakses oleh siapa saja. Hal ini membuka peluang bagi siapa saja yang ingin melakukan kejahatan. Kejahatan yang dimaksud adalah kejahatan yang berkaitan dengan aksesibilitas data atau informasi.

Salah satu data atau informasi yang dapat diakses dengan mudah adalah data berupa citra. Seseorang dapat mengakses dan melakukan pembocoran, pencurian, pemalsuan, dan pengakuan hak milik data atau informasi tersebut. Kejahatan ini dapat merugikan masyarakat di berbagai bidang. Contohnya adalah di bidang kesehatan, yaitu *telemedicine*, *telemedicine* adalah teknologi yang membantu kita untuk melakukan pengawasan kesehatan seseorang pada jarak jauh [1]. Pada proses pengawasan kesehatan tersebut, pertukaran data seperti hasil uji lab atau yang lainnya perlu memiliki tingkat keamanan yang tinggi karena data tersebut berisi informasi pribadi milik pasien yang tidak boleh diakses oleh pihak yang tidak berwenang. Contoh lainnya adalah di bidang *smart surveillance* yang melakukan pengawasan berupa data yang berisikan informasi pribadi seperti wajah [2].

Keamanan data dapat ditingkatkan dengan menggunakan metode enkripsi yang kuat seperti *Advanced Encryption System* (AES) atau *Rivest Shamir Adleman* (RSA) namun metode ini relatif mahal, sedangkan biasanya suatu data tidak seutuhnya bersifat sensitif [2]. Oleh karena itu, penelitian ini mengusulkan sistem keamanan bertingkat. Sistem ini memberikan dua atau lebih level aksesibilitas pada sisi penerima. Dengan demikian, terdapat dua tipe penerima, yaitu penerima yang hanya dapat mengakses bagian nonsensitif dan penerima yang dapat mengakses keseluruhan data termasuk bagian sensitifnya. Sistem ini bekerja dengan mengaburkan bagian sensitif pada citra, tetapi bagian tersebut bersifat reversibel untuk penerima yang berwernang dan memiliki kunci untuk mengembalikan citra yang telah dikaburkan tanpa memanggil kembali citra aslinya [2]. Dengan sistem pengaburan data sebagian ini, keamanan dapat ditingkatkan dengan tanpa menggunakan metode enkripsi yang kuat [2].

Penelitian ini menggunakan metode *visible image watermarking* berbasiskan *Compressive Sensing* (CS). *Image watermarking* adalah teknik menyematkan atau menyisipkan informasi ke dalam sebuah citra [3]. Pada penelitian ini, data yang diambil untuk menjadi *watermark*-nya adalah area wajah. Area wajah tersebut diambil secara otomatis dengan menggunakan algoritma *viola jones*. Selanjutnya, citra wajah yang akan dijadikan *watermark* didekomposisi dengan menggunakan metode *Singular Value Decomposition* (SVD) menjadi sinyal S, U dan V. Setelah itu, sinyal S diambil untuk dilakukan akuisisi dengan menggunakan metode CS sehingga menghasilkan sinyal Y. Kemudian, sinyal Y, U, V dan matriks kompresi A pada proses akuisisi CS disusun kembali sedemikan rupa sehingga ukurannya sama dengan citra wajah asli untuk dijadikan *watermark*. CS adalah metode pengolahan sinyal yang dapat memulihkan sinyal seperti semula dengan hanya menggunakan sampel terbatas yang bersifat jarang dan inkoheren [4]. Proses mengembalikan citra yang telah dikompresi CS disebut rekonstruksi. Pada penelitian ini, metode rekonstruksi yang digunakan adalah *Orthogonal Matching Pursuit* (OMP). Teori

CS menyatakan bahwa sinyal dapat direpresentasikan dengan jumlah sampel sinyal yang jauh lebih sedikit dibandingkan dengan laju *sampling Nyquist* jika sinyal merupakan *sparse signal* atau setidaknya sinyal dapat dikompresi [5]. Teori CS juga mengklaim bahwa proses *sampling* dan kompresi dapat dilakukan secara bersamaan untuk mengurangi laju *sampling* [6]. Selanjutnya, penelitian ini diimplementasikan pada citra dengan wajah sebagai bagian sensitifnya dan berfokus pada proses citra yang sudah dikaburkan namun tetap dapat dikembalikan di sisi penerima yang memiliki kunci. Dengan demikian, penerima yang berwenang tetap dapat mengenali wajah tersebut.

1.2 Penelitian Terkait

Beberapa penelitian yang sudah dilakukan sebelumnya menjadi referensi penelitian ini. Salah satunya adalah penelitian [2]. Penelitian [2] menjadi referensi utama dari penelitian ini karena memiliki tujuan yang sama. Pada penelitian tersebut, perhitungan *Peak Signal-to-Noise Ratio* (PSNR) dan *Structural Similarity Index* (SSIM) dengan laju kompresi atau CS *Measurement Rates* (MR) yang berbeda menjadi parameter kualitas rekonstruksi data di sisi penerima [2]. Hasil dari penelitian [2] menunjukkan bahwa area sensitif yang sudah dikaburkan tidak dapat dikenali oleh penerima yang tidak memiliki otoritas (*User A*) dengan nilai PSNR lebih rendah dari penerima yang memiliki otoritas (*User B*). Hasil terbaik pada penelitian [2] adalah pada saat MR bernilai 0.8 dan kekuatan *embedding* sebesar 0.085 dengan menggunakan *binary masked gaussian*. Nilai PSNR yang dihasilkan untuk area sensitif di *User A* sebesar 11.22 dB dan *User B* sebesar 40.72 dB sedangkan untuk area non-sensitif nilai PSNR di *User A* sebesar 29.73 dB dan *User B* sebesar 43.85 dB. Sementara itu, nilai PSNR yang dihasilkan untuk keseluruhan *frame* di *User A* sebesar 22.11 dB dan *User B* sebesar 42.79 dB. Selain itu, untuk nilai SSIM-nya, data di sisi *User A* dan *User B* menghasilkan nilai SSIM sebesar 0.1770 dan 0.9660 [2].

Selain itu, penelitian terkait yang menyediakan keamanan *multi-level* dengan pendekatan *watermarking* yang kuat adalah penelitian [7]. Penelitian tersebut menggunakan Teknik *Discrete Wavelet Transforms* (DWT), *Discrete Cosine Transform* (DCT) dan SVD sebagai metode *image watermarking*. Sebagai tambahan, keamanan pada penelitian [7] ditingkatkan dengan menggunakan metode *two-dimensional logistic map* berbasiskan *chaotic encryption*. Penelitian [7] menggunakan citra medis sebagai citra *host*-nya. Pada citra medis yang berbeda dengan nilai *gain factor* 0.09, nilai PSNR dan SSIM terbaik adalah pada citra *Computed Tomography Scan* (CT-scan) dengan nilai masing-masing sebesar 35.52 dB dan 0.9991 sedangkan nilai *Normalized Correlation* (NC) terbaik adalah pada citra *Magnetic Resonance Imaging* (MRI) dengan nilai sebesar 0.9989 [7].

1.3 Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan sebelumnya, berikut merupakan rumusan masalah pada penelitian Tugas Akhir ini:

1. Bagaimana sistem keamanan multi-level dapat mempengaruhi aksesibilitas penerima data?
2. Bagaimana sistem yang dirancang dapat mengembalikan informasi citra yang sudah dikaburkan tanpa mengubah informasi citra yang asli?
3. Bagaimana data yang dikaburkan hanya dapat diakses oleh penerima yang memiliki otoritas atas data tersebut?

1.4 Tujuan dan Manfaat

Tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut:

1. Merancang sistem keamanan data menggunakan sistem *multi-level* pada aksesibilitas data dengan mengaburkan sebagian data pada bagian data yang mengandung informasi pribadi, yaitu wajah, yang bersifat reversibel.

2. Merancang simulasi sistem pada *visible image watermarking* dengan menggunakan metode SVD dan CS.
3. Menganalisis performa sistem dengan menggunakan PSNR, SSIM dan NC sebagai parameternya.

Manfaat dari penelitian Tugas Akhir ini adalah sebagai berikut:

1. Memberikan perlindungan data dengan sistem keamanan berlapis.
2. Mengurangi potensi kerugian pemilik data akibat penggunaan data secara tidak resmi.
3. Melindungi keaslian dan hak cipta data dari pihak yang tidak berwenang.

1.5 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan yang telah dibuat, berikut merupakan batasan masalah yang menjadi kondisi-kondisi yang menjelaskan ruang lingkup penelitian Tugas Akhir ini:

1. Data *input* yang digunakan adalah berupa kumpulan citra RGB yang diekstraksi dari sebuah vidio.
2. Data *input* merupakan kumpulan citra berjumlah 199 buah berukuran 1280×720 piksel yang berisikan data pribadi atau sensitif berupa wajah.
3. Data *output* dari sistemnya adalah citra yang bagian sensitifnya sudah dikaburkan dan kunci berupa *txt file* untuk rekonstruksi di sisi penerima yang berwenang.
4. Data sensitif, yaitu wajah, dideteksi secara otomatis dengan menggunakan algoritma *viola jones*.
5. Data sensitif dikaburkan dengan metode dekomposisi menggunakan SVD dan CS untuk disisipkan pada citra *host*.
6. Algoritma rekonstruksi CS yang digunakan adalah metode OMP.

1.6 Metode Penelitian

Pendekatan atau metode yang digunakan dalam proses penyelesaian penelitian Tugas Akhir ini adalah sebagai berikut:

1. Studi literatur

   Mempelajari dan memahami konsep metode yang akan digunakan melalui jurnal, paper dan publikasi ilmiah lainnya yang meneliti topik serupa sebagai rujukan penelitian.

2. Perancangan sistem

   Penelitian ini akan dirancang dan diprogram dengan menggunakan MATLAB untuk proses *watermarking* berbasiskan metode CS pada citra yang diekstrak dari vidio.

3. Simulasi

   Simulasi bertujuan untuk menganalisis keberhasilan program, yaitu dengan melihat hasil *output* program, apabila program sudah dapat mengaburkan informasi pada citra berupa wajah dan dapat mengembalikannya di sisi penerima tanpa mengubah informasi yang asli maka program sudah berhasil.

4. Implementasi

   Hasil dari penelitian ini dapat diimplementasikan pada citra yang mengandung informasi pribadi berupa wajah.

1.7 Sistematika Penulisan

Sistematika penulisan dalam penelitian Tugas Akhir ini adalah sebagai berikut:

Bab I PENDAHULUAN

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

Bab II TINJAUAN PUSTAKA

Di dalam bab ini terdapat penjelasan mengenai konsep dasar yang menunjang

penelitian ini seperti, pengertian dari citra digital, tipe citra digital, *viola jones*, *digital watermarking*, CS dan SVD.

Bab III PERENCANAAN SISTEM

Di dalam bab ini menguraikan model sistem yang telah dirancang oleh penulis beserta diagram alir penelitian, skenario penelitian, dan parameter yang menjadi acuan dari penelitian.

Bab IV ANALISIS SIMULASI SISTEM

Di dalam bab ini memberikan hasil simulasi serta analisis yang sesuai dan dapat dihubungkan dengan konsep dasar dan tujuan awal dari penelitian.

Bab V KESIMPULAN DAN SARAN

Di dalam bab ini merupakan bagian dari penutup penelitian yang berisi kesimpulan dan saran untuk penelitian berikutnya.