Bab 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi pengolahan citra yang sangat pesat, membuat nilai integritas suatu citra perlu dilindungi terutama jika citra tersebut digunakan oleh pihak – pihak tertentu seperti kepolisian dan kedokteran. Pihak yang akan menggunakan citra tersebut harus memastikan bahwa citra yang diterima merupakan data citra yang asli dan belum mengalami modifikasi yang menyebabkan perubahan isi konten dari citra tersebut.

Salah satu cara untuk melindungi nilai integritas suatu citra dengan menggunakan *Media Signature Scheme* (MSS) [1] yang merupakan pengembangan dari skema *Digital Signature Scheme* (DSS). Pada DSS, data yang akan dilindungi diberi fungsi *hash* dan dienkripsi untuk menghasilkan *signature*. Autentikasi kemudian dilakukan dengan membandingkan nilai hasil ekstraksi *signature* dengan nilai data yang diterima. Sementara pada MSS, data yang digunakan untuk dijadikan *signature* adalah nilai hasil ekstraksi fitur dari citra. Pengembangan skema MSS telah banyak dilakukan seperti pada sumber [2],[3],[4] dan [5]. Pemakaian *private* dan *public key* untuk menambah keamanan *signature* juga telah digunakan pada sumber [6]. Penggunaan nilai pada domain frekuensi citra untuk proses ekstraksi fitur telah dilakukan pada sekma sebelumnya. Hasil yang diperoleh dari penggunaan ekstraksi fitur pada domain frekuensi ini menghasilkan performansi autentikasi yang baik pada citra yang mengalami modifikasi yang dilakukan secara sengaja untuk mengubah isi konten citra (*intentional attack*). Namun, pada skema tersebut masih terdapat permasalahan yang masih muncul yaitu berupa autentikasi pada citra yang mengalami serangan yang terjadi tanpa ada tujuan mengubah isi konten citra (*incidental attack*). Pada proses autentikasi, citra yang mengalami *incidental attack* atau serangan yang terjadi tanpa ada kesengajaan, masih dapat dianggap sebagai citra yang autentik. Oleh karena itu, dibutuhkan suatu skema autentikasi yang dapat melakukan identifikasi terhadap citra yang terkena *incidental attack* atau mengalami *intentional attack.*

Untuk dapat memenuhi kebutuhan autentikasi citra tersebut, tugas akhir ini memperkenalkan suatu skema autentikasi berbasis fitur statistik *second-order*. Ekstraksi fitur dilakukan pada domain frekuensi citra dengan membuat matriks ketetanggaan dan menghitung nilai statistik dari matriks ketetanggaan citra tersebut. Untuk menghasilkan *signature*, proses yang dilakukan adalah sama seperti pada skema MSS di mana nilai fitur dari citra tersebut akan diberi fungsi *hash* dan dienkripsi untuk menghasilkan *signature*. Untuk melindungi *signature* tersebut selama pengiriman ke pihak penerima, *signature* tersebut disisipkan ke dalam citra dengan menggunakan teknik *watermarking*. Autentikasi dilakukan dengan membandingkan nilai hasil ekstraksi *signature* dengan nilai fitur citra yang diterima. Apabila suatu citra mengalami *intentional attack,* maka citra tersebut akan teridentifikasi sebagai citra yang tidak autentik. Sementara apabila

citra tersebut mengalami *incidental attack,* maka citra tersebut akan teridentifikasi sebagai citra yang autentik.

1.2. Perumusan Masalah

Hong-Bin Zhang dkk. Telah mengembangkan suatu skema autentikasi dengan menggunakan *invariant* dari koefisien DCT sebagai data yang digunakan untuk menentukan autentik atau tidaknya suatu citra [2]. Skema ini telah berhasil melakukan autentikasi dan perlindungan kepemilikan pada suatu citra. Namun pada skema ini tidak mempertimbangkan serangan yang tidak mengubah makna citra seperti *incidental attack*. Tao Chen dkk. juga telah mengembangkan skema autentikasi dengan memanfaatkan *digital signature* yang dibangkitkan dari *bit pixel* pada setiap blok citra dan memrosesnya dengan filter *low-pass* [3]. Skema ini mampu melakukan autentikasi serta menunjukkan letak modifikasi yang dilakukan. Namun skema ini juga tidak mempertimbangkan jenis serangan berupa *incidental attack*. *Survey* yang dilakukan oleh Jinse dan Christoph pada beberapa skema autentikasi menggunakan teknik *hashing* menghasilkan kesimpulan bahwa skema yang diteliti memiliki nilai ketahanan *robustness* yang baik namun memiliki sensitifitas yang rendah [4]. Skema yang diteliti oleh Jinse dan Christopher memiliki kelemahan dalam melakukan autentikasi pada citra yang mengalami serangan berupa *intentional attack* dengan skala yang kecil. Ekstraksi fitur pada level 2 domain frekuensi DWT telah dikembangkan oleh Chaitanya dkk. [5]. Skema ini menggabungkan nilai *pixel* pada frekuensi rendah tinggi, tinggi rendah dan tinggi tinggi dari citra. Skema ini mampu mendeteksi adanya modifikasi pada citra. Namun pada skema ini, *gaussian dan salt & pepper noise* yang merupakan *intentional attack* masih dianggap sebagai serangan yang mengubah konten citra. Keamanan *watermark* telah ditingkatkan pada skema yang dikembangkan oleh Ping Wah Wong dkk. dengan menggunakan metode enkripsi *secret* dan *public key* [6]. Meskipun skema ini memiliki keamanan yang tinggi dan mampu melakukan autentikasi pada citra dengan baik, skema ini masih tidak mempertimbangkan serangan berupa *incidental attack* yang mungkin terjadi pada citra. Penelitian yang dilakukan pada Shilpi Saha dkk. pada beberapa skema autentikasi dan perlindungan integritas citra menyimpulkan bahwa nilai integritas citra terhadap berbagai jenis serangan masih menjadi permasalahan yang perlu diatasi [7].

Berdasarkan *reference tracing* tersebut, dapat disimpulkan bahwa autentikasi terhadap citra yang mengalami *incidental attack* masih menjadi masalah dalam autentikasi citra. Citra yang mengalami *incidental attack* masih dapat dikategorikan sebagai citra yang autentik karena jenis serangan ini terjadi secara tidak sengaja. Selain permasalahan autentikasi pada citra yang mengalami *incidental attack*. Keamanan *signature* yang digunakan pada proses autentikasi merupakan hal yang harus diperhatikan. Pengiriman *signature* secara terpisah mengandung resiko yang menyebabkan nilai *signature* berubah.

Berdasarkan masalah - masalah tersebut, permasalahan yang akan dibahas pada tugas akhir ini antara lain :

1. Bagaimana melakukan proses autentikasi yang dapat mengidentifikasi citra dengan berupa *incidental attack* sebagai citra yang autentik?
2. Bagaimana melindungi *signature* yang digunakan untuk autentikasi citra?

1.3. Tujuan

Tujuan dari penulisan tugas akhir ini di antaranya adalah :

1. Membangun skema autentikasi dengan memanfaatkan fitur statistik *second-order* untuk melakukan autentikasi terhadap suatu citra yang diterima dan dapat mengidentifikasi citra yang mengalami *incidental attack* sebagai citra yang autentik.
2. Menerapkan teknik *watermarking* untuk melindungi nilai *signature* yang akan digunakan pada proses autentikasi.

1.4. Batasan Masalah

Batasan masalah yang digunakan pada tugas akhir ini antara lain :

1. Format citra yang digunakan pada proses autentikasi berupa .TIFF.
2. Proses penyebaran kunci (*key sharing*) dengan menggunakan protokol *key sharing* untuk enkripsi dan dekripsi antara pihak pengirim dan penerima tidak akan dibahas secara detail pada tugas akhir ini.

1.5. Metode Penyelesaian Masalah

Berikut merupakan metode penyelesaian masalah yang akan dilakukan berkaitan dengan pembuatan skema autentikasi :

a. Identifikasi Masalah

Tahap ini merupakan tahap awal dari perancangan skema. Tahap ini dilakukan dengan menganalisis masalah – masalah yang ada dan akan dijadikan sebagai bahan analisis tugas akhir ini.

b. Studi Pustaka

Studi pustaka dilakukan untuk mencari metode – metode yang dapat digunakan dalam pembangunan skema autentikasi. Kegiatan studi pustaka sendiri bisa dilakukan dengan berbagai cara. Cara yang akan dilakukan dalam pembuatan sistem ini adalah dengan membaca referensi berupa *paper* serta *browsing* di internet.

c. Menentukan Metode Sistem

Penentuan metode ini dilakukan setelah melakukan beberapa penelitian dan pengambilan kesimpulan berdasarkan studi pustaka yang telah dilakukan sebelumnya.

Ada beberapa hal yang perlu dikembangkan dalam menentukan metode yang digunakan. Di antaranya adalah :

1. Tingkat kompleksitas dari metode.
2. Keunggulan metode yang akan diambil dibandingkan dengan metode-metode serupa yang lainnya.
3. Ketahanan metode terhadap serangan-serangan (*incidental* dan *intentional*) yang mungkin terjadi pada citra yang akan diautentikasi.
4. Nilai dari beberapa variabel seperti MSE (*Mean Square Error*) dan (*Peak Signal to Noise Ratio*).

d. Pembangunan *Data Set*

Seluruh *data set* yang digunakan pada pengujian sistem didapatkan dari tahap ini. *Data Set yang digunakan* berupa citra *grayscale* yang diambil dari berbagai sumber di internet dengan ukuran lebar dan tinggi citra yang sama.

Untuk melakukan pengujian kerusakan citra, citra yang telah disisipi *watermark* akan diproses dengan aplikasi pengolahan citra. Proses yang dilakukan berupa pemberian *intentional attack* pada citra ber-*watermark* tersebut.

e. Pembangunan Sistem

Tahap ini merupakan tahap implementasi dari metode yang dipilih. Implementasi ini berupa pembangunan sistem dengan metode yang telah ditentukan pada tahap sebelumnya. Keluaran dari tahap ini berupa skema autentikasi yang digunakan untuk memeriksa apakah citra yang diterima autentik atau tidak.

f. Pengujian Sistem

Tahap ini dilakukan untuk menguji skema yang telah dibuat pada tahap sebelumnya. Pengujian dilakukan untuk mengukur performansi skema autentikasi serta ketahanan skema terhadap berbagai jenis serangan yang mungkin terjadi.

g. Analisis Pengujian

Hasil dari pengujian yang dilakukan di-analisis untuk menilai performansi dari skema yang telah dibuat.

h. Pembuatan Buku Tugas Akhir

Pembuatan buku tugas akhir merupakan tahap akhir dari keseluruhan kegiatan. buku yang dibuat menjelaskan keseluruhan isi dari sistem mulai dari rancangan, metode yang digunakan, serta hasil pengujian dan performansi yang telah dibuat. Dalam laporan juga dituliskan kesimpulan serta saran untuk pengembangan dari sistem yang telah dibuat.