BAB I

PENDAHULUAN

1.1 Latar Belakang

Di jaman digital seperti sekarang telah banyak peranan media seperti sertifikat tergantikan oleh media digital sertifikat. Hal ini di karnakan beberapa kelebihan *digital sertifikat* seperti kemudahan untuk transmisi, penympanan, penyalinan yang sempurna dan kemudahan untuk melakukan pengeditan. Di samping beberapa kelebihan dari digital sertifikat, terdapat kelemahan juga seperti manipulasi yang menyebabkan pelanggaran legalitas dari Media *digital sertifikat*.

Sebagai salah satu solusi perlindungan legalitas dari media *digital sertifikat*, maka *watermarking* dan *kriptografi* digunakan untuk melakukan melakukan legalitas pada media *digital sertifikat*. *Watermarking* yaitu Teknik yang di pakai untuk menyisipkan informasi yang manunjukan kepemilikan atau data lain pada objek multimedia, tapi tidak di ketahui keberadaanya oleh indra manusia dan bisa bertahan dari berbagai serangan yang bermaksud menghilangkan informasi yang di sisipkan [1].

Dinata Training Center adalah Lembaga yang bergerak di bidang training peningkatan Sumber Daya Manusia. Dengan demikian, sebagai Lembaga yang sering mengadakan training dan mengeluarkan *digital sertifikat* pelatihan NLP, Public Speaking dan motivasi yang berguna untuk nilai tambah bagi pelamar saat melamar pekerjaan di perusahaan. Saat ini Dinata Training Center masih menggunakan *digital sertifikat* bisa tanpa di lengkapi pengamanan yang di khawatirkan di manipulasi oleh orang orang tidak bertanggung jawab memanfaatkan kelemahan tersebut.

Untuk itu Dinata Training Center, perlu sistem yang dapat mengamankan *digital sertifikat* dari pemanipulasi *digital sertifikat* dengan proses *encrypt* menggunakan

methode RC6 pada data *Digital sertifikat* dan menggunakan methode LSB pada teks yang sudah di *encrypt* ke image sertifikat.

Watermarking merupakan pengembangan dari *steganografi*. Tapi *watermarking* memiliki perbedaan dari *steganografi*. *Steganografi* aman, sulit di deteksi, dan bisa menampung banyak pesan (*large capacity)* bertujuan menyisipkan pesan rahasia tanpa menimbulkan kecurigaan dan media yang menjadi wadah di sisipkan tidak berarti apa-apa (*meaningless)*[1]. Sedangkan *watermarking* untuk melindungi hak cipta, kepemilikan, sidik jari (*fingerprint)* dan legalitas dari objek wadah yang di sisipi.

Algoritma RC6 yang sederhana dan cepat sehingga mudah diaplikasikan untuk pengamanan data teks menggunakan kunci sehingga data teks tidak dapat di akses oleh orang yang tidak bertanggung jawab[2].

Berdasarkan uraian di atas maka pada penelitian ini mengangkat judul tugas akhir yang berjudul **"Implementasi *Watermarking* Dengan Metode Least Significant Bit Berbasis Kriftografi *Rivest Cipher 6* Untuk Digital Sertifikat"**.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dipaparkan di atas, penulis memiliki beberapa rumusan masalah terkait dengan penelitian ini, yaitu:

1) Bagaimana cara melindungi legalitas dari *digital sertifikat*?
2) Apakah metode LSB *(Least Significant Bit)* dan RC6 *(Rivest Cipher 6)* mampu melindungi legalitas pada *digital sertifikat*?
3) Apakah file sebelum di legalitas dan sesudah di legalitas terdapat perbedaan yang signifikan?
4) Seberapa kuat file yang sudah di legalitas terhadap cropping dan editing?

1.3 Tujuan Penelitian

Adapun tujuan dari pembuatan tugas akhir ini yaitu :

1) Merancang dan membangun aplikasi *watermarking* untuk melindungi legalitas dari *digital sertifikat*.
2) Menerapkan Teknik *watermarking* methode LSB *(Least significant Bit)* dan *kriftografi* methode RC6 *(Rivest Cipher 6)* dalam melindungi *digital sertifikat*.
3) Melakukan perbandingan file yang sudah di legalitas dan yang sebelum legalitas.
4) Melakukan pengujian ketahanan dari file digital sertifikat yang sudah di legalitas.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian **Implementasi** *Watermarking* Dengan Metode Least Significant Bit Berbasis Kriftografi *Rivest Cipher 6* Untuk Digital Sertifikat adalah untuk menyisipkan nomor seri yang sudah di enkripsi dan menyisipkanya ke dalam gambar atau file, sertifikat sehingga mencegah terjadinya kepalsuan, manipulasi dan penipuan pada sertifikat.

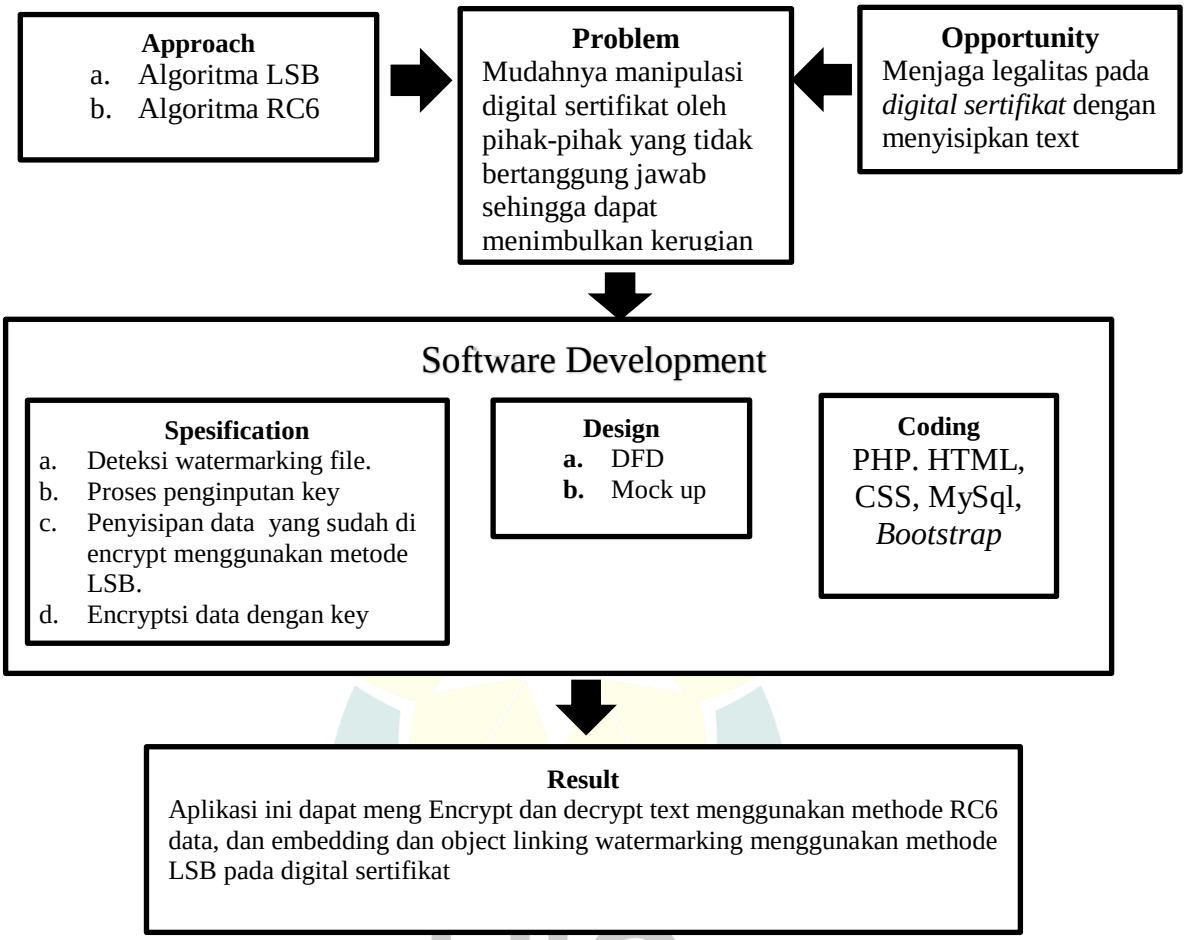
1.5 Batasan Masalah

1. Pemrograman yang digunakan adalah berbasi *web.*
2. Metode *kriptografi* yang digunakan adalah metode *RC6.*
3. Metode watermarking yang digunakan adalah metode *LSB*
4. File yang di sisipkan berupa Text.
5. File citra yang digunakan berupa PNG atau JPG.

1.6 Kerangka Pemikiran

Kerangka pemikiran merupakan uraian tentang bagaimana peneliti mengalirkan jalan pemikiran secara logis dalam rangka memecahkan masalah yang telah di rumuskan dimulai dari permasalahan yang ada pada penelitian ini, lalu opportunity untuk memecahkan permasalahan, approach methode atau algoritma yang di gunakan, tahapan software development yang di dalamnya adaspesipikasi kebutuhan, rancangan desain, dan

coding, dan menghasilkan sebuah aplikasi yang dapat memecahkan masalah yang dihadapi. Dan berikut alurnya:



Gambar 1.1 Skema Kerangka Pemikiran

1.7 Metodologi Pengerjaan Tugas Akhir

1.7.1 Tahap Pengumpulan Data

Untuk mengumpulkan berbagai data yang di butuhkan untuk kelancaran penyusunan tugas akhir ini ada tahap tahap yang perlu di lakukan sebagai berikut:

1. Wawancara (interview)

   Melakukan survei terhadap beberapa orang untuk mencari kekurangan dari *digital sertifikat* dan tanya jawab dengan Dinata Training Center untuk menentukan kebutuhan apa saja yang perlu di terapkan.

2. Studi Literatur

Metode pengumpulan data dalam penelitian ini adalah studi Pustaka yaitu pengumpulan data dengan cara mengumpulkan materi-materi literatur dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, situs di internet dan bacaan-bacaan yang berkaitan dengan judul penelitian.

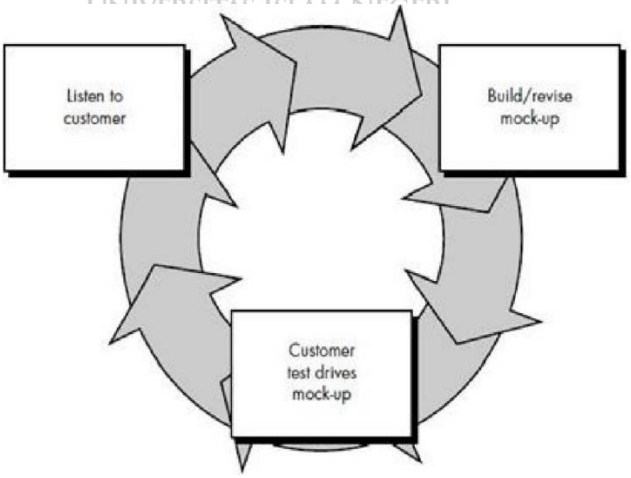
3. Pemodelan Sistem

Dalam pemodelan sistem dilakukan perancangan aplikasi menggunakan methode *Unified Modeling Language* (UML), kemudian di implementasikan pada pembangunan aplikasi berbasis *web*.

4. Model Proses Pengembangan Perangkat lunak

Metode pengembangan perangkat lunak yang digunakan pada penelitian ini yaitu menggunakan metode *prototype*. *Prototyping* merupakan salah satu metode pengembangan perangkat lunak yang banyak digunakan. Dengan metode *prototyping* ini pengembang dan pelanggan dapat salingberinteraksi selama proses pembuatan sistem.

Gambar dibawah ini menunjukkan secara keseluruhan arsitektur yang dimiliki *prototype.*



Gambar 1.2 Arsitektur *Prototype* [3]

Adapun tahapan dalam siklus pegembangan *prototype* yaitu:

1. Analisis kebutuhan. Tahap analisis kebutuhan (*requirements*) dilakukan untuk mengidentifikasi tentang siapa yang akan menggunakan sistem dan apa yang dibutuhkan oleh pengguna dari sistem.
2. Perancangan sistem. *System design* atau perancangan sistem merupakan tahap dimana sistem digambarkan ke dalam model- model tertentu berdasarkan hasil analisis pada tahap sebelumnya.
3. Pengkodean. Untuk membangun sistem ke dalam bentuk asli, maka hasil perancangan diterjemahkan ke dalam kode-kode tertentu.
4. Pengujian. Pengujian (*testing*) perlu dilakukan dalam setiap pengembangan sistem. Tujuannya yaitu untuk mengukur apakah sistem yang telah dikembangkan berjalan dengan baik dan benar serta sesuai dengan kebutuhan pengguna.
5. Implementasi Setelah semua tahap berjalan dengan baik dan hasil pengujian menunjukkan hasil yang sesuai dengan kebutuhan, maka sistem dapat diimplentasikan dan siap digunakan oleh pengguna dengan tetap melakukan pemeliharaan (*maintenance*) secara berkala untuk menjaga kesehatan *system*.

1.8 Sistematika Penulisan

Sistematis penulisan penelitian ini di bagi menjadi (5) bab yang masing masing bab sudah mempunyai tujuan-tujuan masingmasing. Berukit penjelasanya :

BAB I PENDAHULUAN

Bab I (satu) pendahuluan yang berisi pembahasan permasalahan yang berhunungan drnagan penysunan laporan tugas akhir diantaranya latar belakang, rumusan masalah, Batasan masalah, sistematika penulisan, tujuan dan manfaat penelitian.

BAB II LANDASAN TEORI

Bab II (dua) landasan teori menjelaskan teori-teori yang berhubungan dengan masalah yang di kemukakan dapa penelitian ini, dan juga teori-teori yang di gunakan dalam perancangan dan implementasi.

BAB III METODELOGI PENELITIAN

Bab III (tiga) ini membahas mengenai metode penelitian dan kebutuhan perangkat lunak dan perangkat keras yang di gunakan.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab IV (empat) disini di bahas car acara penyajian Teknik inplementasi serta pengujian sistem yang sudah selesai, termasuk preview dari hasil akhir pada aplikasi.

BAB V PENUTUP

Bab V (lima) berisi kesimpulan dan saran guna untuk pengembangan aplikasi ke tahapan lebih lanjut dalam upaya untuk memperbaiki dan pengembangan aplikasi sebih baik.

DAFRAT FUSTAKA

Daftar Pustaka berisi semua sumber tertulis atau tercetak yang pernah di kutip dan di gunakan pada proses penyusunan.

LAMPIRAN

Berisi semua dokumen yang di gunakan dalam proses penyusunan dan perancangan seperti source code, kelengkapan dokumen dan lain sebagainya.