BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

House The House adalah salah satu konsultan *art* dan *design* di Bandung. Perusahaan ini menangani beberapa pekerjaan yang berhubungan dengan desain seperti *branding*, perencanaan dan desain bangunan, penelitian dan hiburan. Perusahaan ini memiliki lebih dari 8 pekerja dengan jumlah proyek yang pernah ditangani 30 branding, 4 desain interior dan 40 kegiatan serta pernah mendapatkan penghargaan *"Shell LiveWIRE Indonesia Business Start-Up Awards 2013"*.

Dilihat dari prestasi yang telah didapatkan tersebut tentu saja banyak klien yang meminta pihak House The House untuk menjadi desainer mereka. Setelah dilakukan wawancara langsung dengan CEO dari House The House didapatkan sebuah informasi bahwa dari beberapa klien tidak semuanya melanjutkan kerjasama mereka setelah mendapatkan desain dari pihak House The House. Namun dari informasi yang didapatkan pihak House The House bahwa klien yang tidak melanjutkan kerjasama dengan pihak House The House tersebut tetap menggunakan desain mereka. Jika kasus tersebut terus terjadi maka akan mengakibatkan kerugian besar untuk pihak House The House mengingat dalam dunia desain konsep suatu desain itu sangat berharga. Meskipun pada implementasinya suatu desain mengalami perubahan namun dengan konsep yang sama tentu bisa dikatakan tetap menggunakan konsep dari pihak House The House.

Berdasarkan kasus yang ada maka diperlukan sebuah aplikasi untuk mengamankan gambar di perusahaan House The House tersebut. Dalam hal ini khususnya untuk membatasi klien untuk melihat desain agar mengurangi penggunaan tanpa izin oleh klien. Salah satu caranya adalah dengan cara menyamarkan gambar digital sehingga tidak bisa dilihat tanpa menggunakan kode dari pihak perusahaan. Untuk hal itu penelitian kali ini akan menggunakan pengamanan dengan teknik kriptografi yang dapat menyamarkan gambar digital menggunakan metode *Rivest-Shamir-Adleman* dengan *Chinese Remainder Theorem* (RSA-CRT). Metode RSA-CRT dipilih karena berdasarkan hasil penelitian Rini Wati Lumbangaol [1] bahwa RSA bisa digunakan untuk enkripsi gambar. Namun berdasarkan buku Kriptografi Untuk Keamanan Jaringan [2] dikatakan bahwa metode RSA membutuhkan waktu lebih lama dalam proses dekripsi sehingga ditambahkan teorema CRT untuk mempercepat proses dekripsi tersebut.

Dengan demikian maka penelitian ini akan berfokus untuk membangun aplikasi keamanan yang berjudul "Penerapan Kriptografi Menggunakan Metode Rivest-Shamir-Adleman dengan Chinese Remainder Theorem (RSA-CRT) Pada Citra Digital Di Konsultan Art dan Design House The House".

Diharapkan dengan penelitian ini akan mengurangi kasus yang terjadi. Selain itu juga dengan teknik kriptografi ini juga dapat mengurangi kemungkinan pihak selain klien dan perusahaan untuk melihat desain yang dibuat.

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang masalah diatas, masalah-masalah yang ada dapat diidentifikasi sebagai berikut :

1. Belum ada pembatasan hak akses untuk melihat citra digital.
2. Pihak klien dapat melihat gambar berulang kali sehingga bisa digunakan pihak klien untuk kepentingan lainnya.

1.3 Maksud dan Tujuan Penelitian

Maksud dari penelitian ini adalah untuk menerapkan kriptografi dengan metode rivest-shamir-adleman dengan chinese remainder theorem RSA-CRT pada citra digital di konsultan *art and design House The House.*

Adapun beberapa tujuan yang ingin dicapai melalui penelitian ini antara lain adalah sebagai berikut :

1. Membuat pembatasan hak akses untuk melihat citra digital.
2. Memberikan batas pada citra untuk dilihat oleh pihak klien.

1.4 Batasan Masalah

Dalam penelitian ini ditetapkan beberap batasan masalah, diantaranya sebagai berikut :

1. Pengolahan foto hanya dilakukan pada citra berwarna 24bit.
2. Format foto yang bisa dilakukan enkripsi yaitu .jpg dan .bmp
3. Aplikasi pengolahan citra menggambarkan proses kriptografi citra saja yaitu proses enkripsi dan dekripsi.
4. Proses enkripsi dan dekripsi menggunakan metode kriptografi RSA - CRT
5. Aplikasi ini akan menghasilkan sebuah *chipertext* dengan format file .jpg
6. Aplikasi ini merupakan aplikasi desktop yang berjalan pada Sistem Operasi Windows.

7. Target pengguna adalah *Konsultan Art and Design House The House* dan kliennya.
8. Pemodelan data pada penelitian ini menggunakan pemodelan terstruktur.
9. Aplikasi ini dibangun menggunakan bahasa pemrograman C# dengan aplikasi Visual Studio 2013

1.5 Metodelogi Penelitian

Metode penelitian akan menggunakan metode kualitatif. Metode penelitian kualitatif merupakan suatu metode yang penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, tindakan dan lain sebagainya. Secara holistik, dan dengan cara deskripsi dalam bentuk kata - kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan bebagai metode alamiah [3].

Secara singkat dapat dijabarkan bahwa metode penelitian kualitatif merupakan metode yang didasarkan pada kasus khusus sehingga pengumpulan dan analisis data bersifat khusus pula [4].

Karena sifatnya yang bersifat khusus itu maka metode penelitian kualitatif sering digunakan dalam berbagai *research*, meskipun beberapa kalangan menolak metode ini karena dianggap tidak bisa mewakili sifat umum penelitian. Namun metode ini tetap saja digemari karena pada prinsipnya bahwa teori yang berkembang perlu menyesuaikan dengan keadaan lingkungannya.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang akan digunakan berdasar metode yang digunakan maka diperoleh beberapa teknik pengumpulan data [4] sebagai berikut :

1. Observasi

Metode pengumpulan data ini dilakukan dengan cara pengamatan langsung kepada objek yang diteliti. Dalam hal ini observasi yang dilakukan melalui beberapa cara sebagai berikut :

a. Melalui wawancara langsung

   Wawancara langsung ini dilakukan untuk memperoleh informasi mengenai latar belakang perusahaan, pekerjaan yang dilakukan, masalah yang ada dan hal lain yang berkaitan dengan penelitian.

b. Melalui pengamatan kerja

Dalam hal ini juga dilakukan pengamatan mengenai cara pekerja melakukan penyimpanan gambar, pengiriman dan beberapa perlakuan lain terhadap objek gambar.

2. Studi Dokumentasi

Metode studi dokumentasi ini sering juga disebut dengan metode studi pustaka. Metode ini dilakukan dengan mencari informasi pada catatan tertulis/gambar yang berkaitan dengan masalah yang diteliti. Dalam penelitian ini diambil beberapa dokumentasi seperti jurnal, laporan peneletian sebelumnya, dokumen perusahaan, buku referensi, *proceding* dan beberapa informasi tertulis dari internet.

Metode ini penting untuk membantu menyusun teori dan validasi data. Dengan teori yang cukup memadai dan data yang valid diharapkan penelitian yang dilakukan dapat memberikan hasil yang sesuai dengan bidang keilmuwan yang ada.

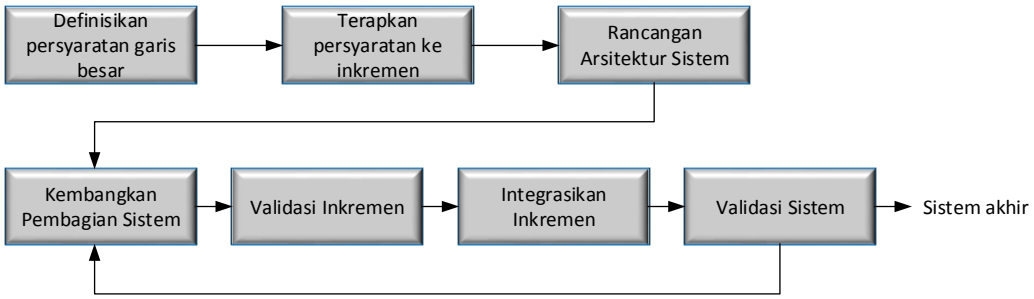
1.5.2 Metode Pembangunan Perangkat Lunak

Metode Pembangunan Aplikasi, melalui metode inkremental yaitu metode yang menggabungkan elemen-elemen model sekeunsial linier (diaplikasikan secara berulang) dengan filosofi prototipe iteratif. Model inkremental menggunakan urutan-urutan linier di dalam model seiring dengan laju waktu kalender [5].

Pada proses pengembangan inkremental, pelanggan mengidentifikasi, secara garis besar, layanan (*service*) yang akan disediakan oleh sistem. Mereka mengidentifikasi layanan mana yang paling penting dan mana yang tidak penting. Bagian-bagian yang harus diserahkan kemudian diidentifikasi, dengan setiap inkremen(bagian) memberikan sebagian dari fungsionalitas sistem. Alokasi layanan pada inkremen bergantung pada prioritas layanan. Layanan dengan prioritas tertinggi dikirimkan terlebih dahulu kepada pelanggan [6].

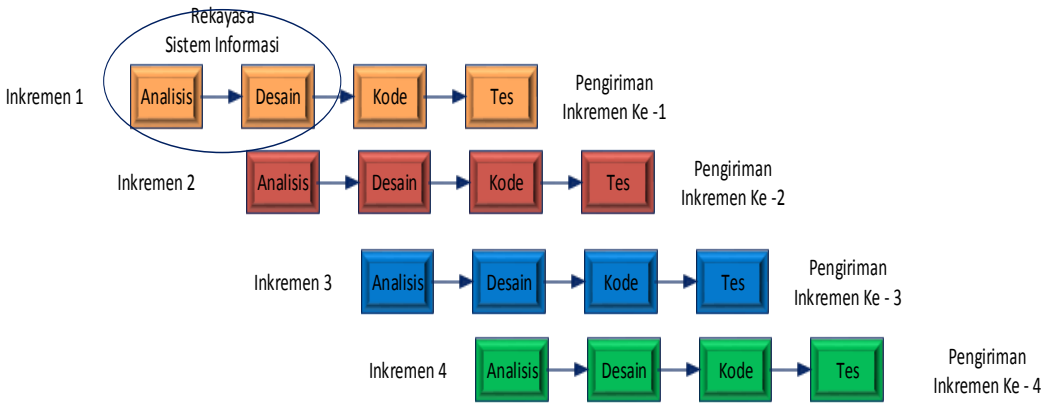
Setiap bagian akan menyerahkan fungsional utama ke bagian lain dan kemudian bagian tersebut akan melakukan pekerjaan untuk fungsionalitas tambahan yang dirasa perlu. Sehingga analisis untuk persyaratan inkremen lainnya bisa dikerjakan namun perubahan persyaratan tidak dapat diterima.

Menurut Ian Sommerville pengembangan inkremental dapat digambarkan sebagai berikut [6] :



Bagan 1.1 Pengembangan Inkremental [6]

Sedangkan menurut Roger S. Pressman [5] berdasar proses yang dilakukan model inkremental ini bisa digambarkan sebagai berikut :



Bagan 1.2 Model Inkremental berdasar waktu kalender [5]

Adapun penjelasan setiap tahapnya sebagai berikut :

a. Analisis

Pada bagian ini akan disusun proses bisnis yang terjadi, analisis kebutuhan pengguna dan pengumpulan data yang berkaitan dengan penelitian ini.

b. Desain

Pada tahapan ini akan dilakukan perancangan aplikasi berdasarkan kebutuhan dari pengguna. Desain dilakukan bertahap sesuai dengan prinsip model inkremental yaitu melakukan desain terhadap kebutuhan utama. Dalam penelitian ini desain akan menggambarkan proses yang akan terjadi, rancangan antarmuka dan detail algoritma prosedural.

c. Kode

Pada langkah ini akan dituliskan kode program berdasarkan rancangan yang telah ditetapkan sebelumnya. Dalam tahapan ini desain akan ditransformasikan ke bentuk bahasa pemrograman.

d. Tes

Pada tahapan tes ini akan diuji menggunakan *black box* yaitu akan diuji fungsionalitas dari program.

e. Pengiriman

Proses pengiriman ini bukan tahapan utama dari pembuat aplikasi. Tahap ini untuk mengetahui kesesuaian fungsionalitas dari aplikasi. Dalam model inkremental fungsionalitas utama akan dikirimkan pada tahap awal. Ini menentukan apakah aplikasi sudah sesuai atau belum sedangkan fungsionalitas bukan prioritas di kirimkan dalam tahap selanjutnya. Pada model inkremental iterasi ini tidak terbatas. Hal ini bisa saja dalam pengiriman pertama fungsionalitas sudah sesuai sehingga iterasi hanya berjalan sekali namun bisa juga dilakukan berkali-kali. Hal ini sesuai dengan perencanaan tahapan setiap inkremennya dan hasil review dari pelanggan dalam hal ini konsultan *Art and Design House The House.*

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran secara umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Pada bab pendahuluan ini, penulis menguraikan tentang secara singkat tentang latar belakang masalah, rumusan masalah, maksud dan tujuan disusunnya penulisan skripsi ini serta batasan-batasan yang digunakan untuk menyelesaikan penulisan skripsi ini. Serta menguraikan pula tentang metodologi penelitian yang digunakan serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bab ini, akan dibahas mengenai teori-teori yang berkaitan dengan judul dari penulisan skripsi ini. Digunakan untuk dapat membantu menyelesaikan setiap tahapan yang dilalui. Seperti teori tentang citra digital, kriptografi, kriptografi RSA-CRT, model sistem, DFD dan bahasa pemrograman yang digunakan.

BAB 3 ANALISIS DAN PERANCANGAN

Berisi analisis kebutuhan untuk sistem yang akan dibangun sesuai dengan metode pengembangan perangkat lunak yang digunakan. Selain itu, bab ini juga berisi perancangan

struktur antar muka untuk aplikasi yang akan dibangun dan pembangunan aplikasi kriptografi dengan menggunakan metode RSA-CRT pada citra digital.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi implementasi dari hasil analisis dan perancangan aplikasi kriptografi dengan menggunakan metode RSA-CRT pada citra digital yang telah dibuat, disertai juga dengan hasil pengujian dari aplikasi kriptografi dengan menggunakan metode RSA-CRT pada citra digital sehingga diketahui apakah aplikasi yang dibangun dapat bermanfaat untuk mengamankan citra digital.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari penelitian yang dilakukan dan juga berisikan tentang saran yang nantinya diperlukan untuk pengembangan aplikasi dari hasil penelitian ini.