PROTEKSI KEAMANAN DOKUMEN SERTIFIKAT FILE JPEG PADA PERGURUAN TINGGI DENGAN MENGGUNAKAN STEGANOGRAFI DAN KRIPTOGRAFI

Ary Budi Warsito[1], Lusi Fajarita[2], Nazori AZ[3]

[1]Teknik Informatika STMIK Raharja
ariebhewhe@gmail.com

[2,3]Magister Ilmu Komputer Program Pascasarjana Universitas Budi Luhur
[2]lusifajar@yahoo.com, [3]nazori@budiluhur.ac.id

ABSTRAK

Proses pengamanan informasi dapat dilakukan dengan menyembunyikan informasi tersebut pada media lain atau dengan metode tertentu, sehingga orang lain tidak menyadari ada suatu informasi didalam media tersebut. Dikenal dengan teknik Steganografi dan Kriptografi. Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Sedangkan kriptografi menyamarkan arti dari suatu pesan, tetapi tidak menyembunyikan bahwa ada suatu pesan. Dalam perguruan tinggi tidak lepas dengan adanya penerbitan dokumen sertifikat. Selain dokumen sertifikat dalam bentuk paper atau hardcover, terdapat juga sertifikat yang diterbitkan secara online. Setiap sertifikat dalam bentuk hardcover memiliki nomor seri atau kode yang unik atau stamp dan tanda tangan dari pejabat yang bersangkutan, sehingga untuk membuktikan keasliannya sangatlah mudah, dibandingkan dengan sertifikat online. Bagaimana cara membuktikan keaslian sertifikat online tersebut? Bagaimana jika stakeholder meminta aslinya padahal sertifikat tersebut dibuat secara online? Apakah pemilik dapat menyakinkan stakeholder bahwa sertifikat ini adalah asli? Oleh karena itu sebuah perguruan tinggi memerlukan media untuk membuktikan keabsahan sertifikat yang dikeluarkan secara online. Penulis telah merancang sebuah aplikasi dengan perpaduan teknik steganografi dan kriptografi untuk menguji keabsahan dari sertifikat tersebut.

Kata Kunci : Steganografi, Kriptografi, sertifikat, keabsahan, pembuktian

1. Pendahuluan

Pertukaran informasi melalui media internet merupakan salah satu keuntungan yang diperoleh dari berkembangnya teknologi saat ini. Bagaimana menjaga kemanan data yang dikirim serta menjamin keabsahan data yang diterima merupakan salah satu yang menjadi tujuan utama. Dalam dunia komputer, ada 2 istilah teknik keamanan data yang sangat dikenal yaitu steganografi dan kriptografi.

Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Sedangkan Kriptografi menyamarkan arti dari suatu pesan, tetapi tidak menyembunyikan bahwa ada suatu pesan. Secara teori, semua file yang ada didalam komputer dapat digunakan sebagai media penampung pesan, seperti file citra berformat JPG, GIF, BMP, file audio berformat MP3, WAV, bahkan didalam sebuah video dengan format AVI, atau dalam format lainya seperti TXT, HTML, PDF.

Ddalam sebuah perguruan tinggi tidak lepas adanya penerbitan dokumen sertifikat. Jika dokumen sertifikat yang dikeluarkan

dalam bentuk *paper* atau *hardcover* mungkin tidak akan menjadi kendala karena bentuk fisik nyata dan dapat dibuktikan keaslianya karena ada *stamp* dan tanda – tangan. Lain cerita jika penerbitan itu di lakukan secara online, Artinya para pemilik sertifikat tersebut mengunduh melalui media Internet. Apa yang akan menjadi bukti keaslian sertifikat tersebut di keluarkan oleh sebuah perguruan tinggi? Bagamaina jika *stakeholder* meminta aslinya padahal sertifikat tersebut dibuat secara online? Apakah pemilik tersebut dapat menyakinkan kepada *stakeholder* tersebut bahwa sertifikat ini adalah asli? Oleh karena itu sebuah perguruan tinggi memerlukan media untuk membuktikan keabsahan sertifikat yang dikeluarkan secara *online*.

Dengan adanya teknik steganografi yang melakukan penyamaran pada media yang di bawah dan kriptografi yang mempunyai tugas sebagai kunci acak maka sertifikat yang dikeluarkan oleh perguruan tinggi dapat dibuktikan.

2. Tujuan

Tujuan dari penelitian ini adalah merancang suatu sistem atau aplikasi dengan menggunakan teknik steganografi dan kriptografi yang digunakan untuk enkripsi dan menguji keabsahan data digital terutama sertifikat penting pada perguruan tinggi dalam bentuk file JPEG. Sehingga antara *stakeholder* dan Pemilik sertifikat akan merasa aman karena pihak tersebut cukup *online* dan *upload* file dalam *web* perguruan tinggi untuk menguji keaslian sertifikat.

3. Batasan Masalah

Agar permasalahan yang dibahas ini tidak keluar dari jalur yang sudah ditentukan maka perlu adanya pembatasan masalah, Batasan masalah tersebut adalah:

1) Implementasi teknik steganografi untuk mengamankan data digital sertifikat dalam bentuk file JPEG
2) Implementasi teknik kriptografi untuk mengetahui isi pesan dari data digital sertifikat dengan metode *decrypt*

4. Teori Dasar

Dalam dunia komputer, ada 2 istilah teknik keamanan data yang sangat dikenal yaitu steganografi dan kriptografi.

a. Steganografi

Dalam [1] Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata "steganografi" berasal dari bahasa Yunani **"*steganos*"**, yang artinya "tersembunyi atau terselubung", dan **"*graphein*"**, "menulis".

Sebuah pesan steganografi (*plaintext*), dienkripsikan dengan beberapa arti tradisional, yang menghasilkan *ciphertext*. Kemudian, *covertext* dimodifikasi dalam beberapa cara sehingga berisi *ciphertext*, yang menghasilkan *stegotext*. Contohnya, ukuran huruf, ukuran spasi, jenis huruf, atau karakteristik *covertext* lainnya dapat dimanipulasi untuk membawa pesan tersembunyi. Hanya penerima (yang harus mengetahui teknik yang digunakan) dapat membuka pesan dan mendekripsikannya. Format yang biasa digunakan dengan menggunakan teknik steganografi diantaranya:

1) Format *image* : bitmap (bmp), gif, pcx, jpeg, dll.
2) Format audio : wav, voc, mp3, dll.
3) Format lain : teks file, html, pdf, dll.

b. Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*) "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan).

Para pelaku atau praktisi kriptografi disebut *cryptographers*. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut *cipher*, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Data yang dienkripsi dapat disandikan dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*).

c. Perbedaan Steganografi dan Kriptografi

Steganografi dan kriptografi mempunyai prinsip kerja yang berbeda, meskipun keduanya mempunyai hubungan yang dekat dalam dunia keamanan data. Hasil dari kriptografi biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi), sedangkan hasil keluaran dari steganografi memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses.

5. Metodologi Penelitian

5.1 Fase Analisis

Studi Literatur

Studi ini dilakukan dengan cara mencari sekaligus mempelajari beberapa literatur dan artikel mengenai steganografi dan kriptografi sebagai acuan dalam perencanaan dan pembuatan sistem atau aplikasi.

a) Pendefinisian dan analisis masalah untuk mencari solusi yang tepat
b) Studi Pustaka

5.2 Fase Pembuatan Program

Perancangan dan implementasi sistem yang dilakukan secara ekperimental, yaitu bereksperimen membuat program berdasarkan materi dan algoritma yang telah dipelajari.

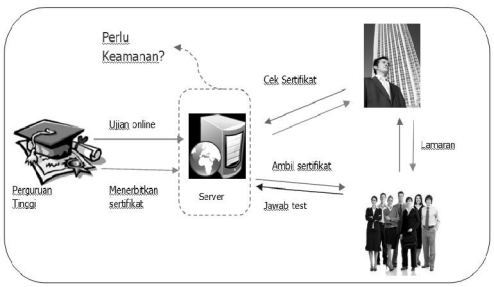
5.3 Pengujian Program

Pengujian dilakukan terhadap program yang telah dibuat.

6. Pola Pikir

6.1 Analisa permasalah dan pemecahannya

Dengan banyak aplikasi atau *tool software* desain grafis dan foto *editing* yang beredar di pasaran maka sangat rentan sekali sertifikat dipalsukan. Dan bagaimana bentuk pertanggungjawaban sebuah perguruan tinggi untuk menjamin bahwa sertifikat yang dikeluarkan tersebut benar-benar asli dikeluarkan dari perguruan tinggi yang bersangkutan. Jika kasusnya adalah sertifikat itu nyata dalam artian *hardcover*, sehingga untuk menguji keasliannya pasti ada ciri khusus atau tanda atau kode rahasia yang hanya pihak perguruan yang mengeluarkan sertifikat yang dapat mengetahui. Bagaimana jika kasusnya adalah sertifikat yang diterbitkan secara *online* sehingga pemilik sertifikat tersebut cukup melakukan unduh sertifikat? Bagaimana sertifikat yang diterbitkan secara online tersebut dapat dicek keaslianya? Berdasarkan kasus tersebut perlu rancangan sistem yang dapat melakukan fungsi tersebut, sehingga sebuah keaslian sertifikat dapat dipertanggungjawabkan. Berikut ini disampaikan ilustrasi permasalahan yang dialami pada sertifikat yang diterbitkan secara online.



Gambar 1. Ilustrasi Sertifikat online

Untuk menjawab permasalah tersebut kita perlu mempelajari permasalah yang

sudah ada dari penelitian sebelumnya agar hasil akhirnya dapat memecahkan permasalahan yang ada. Studi ini dilakukan dengan cara mencari sekaligus mempelajari beberapa literatur dan artikel mengenai steganografi dan kriptografi sebagai acuan dalam perencanaan dan pembuatan sistem atau aplikasi. Dalam upaya pengembangan penelitian ini perlu dilakukan studi pustaka sebagai salah satu dari penerapan metode penelitian yang akan dilakukan. Diantaranya adalah mengidentifikasikan persamaan dari steganografi dan kriptografi, mengidentifikasikan metode yang pernah dilakukan, meneruskan penelitian sebelumnya, serta mengetahui orang lain yang spesialisasi dan area penelitiannya sama di bidang ini. Beberapa *Literature review* tersebut adalah sebagai berikut:

a. Penelitian yang membahas mengenai Algoritma yang digunakan untuk menentukan kekuatan dari enkripsi. Keamanan sebuah algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut "*restricted algorithm*". Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu) [1].
b. Penelitian yang menggunakan metode LSB *(Least Significant Bit)* dan EOF *(End of File)*. Pada penelitian ini, dijelaskan bahwa metode LSB bekerja dengan cara menambahkan bit data yang akan disembunyikan (pesan) di bit terakhir yang paling cocok atau kurang berarti. Sehingga jika dilihat berdasarkan ukuran *stego image* LSB lebih baik karena tidak mengubah ukuran file yang disisipi, namun untuk kualitas *image*, LSB banyak mengurangi kualitas *image* yang semula. Sedangkan cara kerja metode EOF adalah dengan menambahkan data atau file yang akan disembunyikan lebih dari ukuran file *image*. Data yang disembunyikan tersebut akan disisipkan pada akhir file sehingga file *image* akan terlihat sedikit berbeda dengan aslinya. Ada penanda khusus yang terlihat dari file *image* di paling bawah seperti garis-garis. Sehingga Untuk kualitas *image,* EOF lebih baik karena kualitas *image* tetap terjaga, namun ukuran file lebih besar dari sebelum disisipi oleh pesan [2].

Tabel 1. Tabel Hasil Perbandingan Ukuran *Stego Image*

No	Metode	Size Image	Size Pesan	Stego Image
1	LSB	150x200	422 karakter	150x200
2	EOF	150x200	422 karakter	153x200

c. Penelitian yang membahas aplikasi steganografi dengan metode LSB yang melukan penyisipan berbagai jenis data dengan ekstensi yang berbeda. Ukuran dari file bitmap setelah disisip (*Stego Bitmap*) tidak mengalami perubahan dari ukuran file bitmap sebelumnya (*Cover Bitmap*). Metode LSB juga dapat melakukan manipulasi BPC (*Bit Per Channel*) untuk meningkatkan daya tamping cover bitmap semaksimal mungkin. Dengan metode LSB, efisiensi waktu enkripsi dan dekripsi yang relatife cepat dan integritas data sebelum dan sesudah proses ekstrak tidak mengalami perubahan sama sekali [3].
d. Penelitian yang membahas masalah pada kelemahan pada kriptografi pada *encoding* [4].

Dari *Literature review* yang diutarakan di atas kami dapat menarik sebuah titik terang untuk memecahkan permasalahan

yang sedang kami hadapi dengan teknik steganografi dan kriptografi. Kedua teknik ini dapat diterapkan pada sebuah sertifikat dokumen yang diterbitkan secara online. Jika konsep ini akan diterapkan pada perguruan tinggi maka perlu pengelompokan terlebih dahulu jenis dari sertifikat tersebut. Jenis sertifikat tersebut menjadi 2 jenis kebutuhan yaitu:

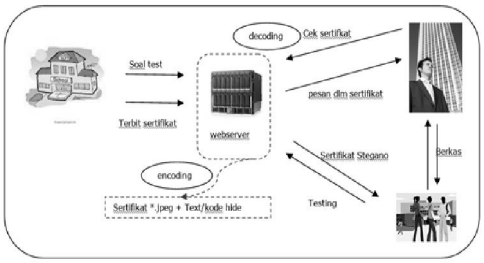
1) Sertifikat penting.

Jenis sertifikat ini adalah sebuah sertifikatnya yang penting pagi pemilik sertifikat tersebut untuk digunakan sebagai pelengkap. Jika terjadi kehilangan pada sertifikat ini maka pemilik sertifikat tersebut tidak mengkhawatirkan. Contoh: sertifikat seminar, sertifikat *workshop*, dll.

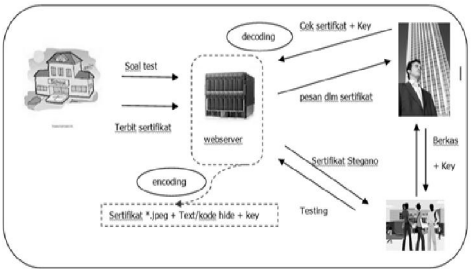
2) Sertifikat sangat rahasia.

Sertifikat ini sangat penting bagi sesorang yang ingin kerahasiaan tersebut terjamin. Sehingga proteksi terhadap sertifikat ini lebih besar dari pada sertifikat penting.

Dari jenis kebutuhan tersebut dan digabungkan dengan Steganografi dan kriptografi makan konsep yang terjadi adalah untuk dokumen yang penting maka cukup dengan melakukan steganografi sebagai bukti keaslian sebuah dokumen yang diterbitkan oleh perguruan tinggi. Sedangkan jika sertifikat tersebut sangat rahasia maka untuk steganografi dan kriptografi berkolaborasi. Untuk lebih jelasnya tentang permasalahan di atas maka penjelasannya dapat digambarkan pada gambar 2 dan gambar 3 sebagai berikut:



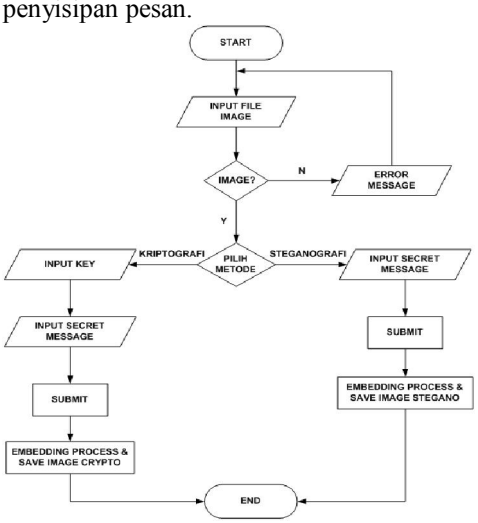
Gambar 2. Ilustrasi Sertifikat Penting



Gambar 3. Ilustrasi Sertifikat Rahasia

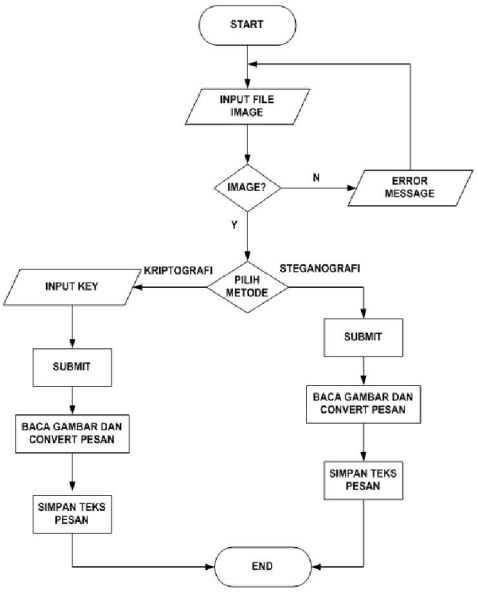
7. Algoritma

Setelah tahapan pola pikir dan alur dari konsep sudah didapat maka di sini akan diperlihatkan algoritma dari aplikasi yang sesuai dengan rancangan di atas. Berikut adalah gambar *flowchart* saat proses penyisipan pesan.



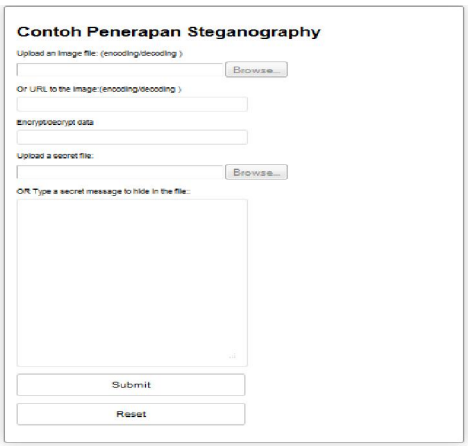
Gambar 4. *Flowchart Embedding*

Berikut adalah gambar *flowchart* untuk mengembalikan pesan teks yang disisipkan, sehingga menghasilkan pesan teks dari gambar.



Gambar 5. Flowchart Ekstraksi

8. Hasil Percobaan



Gambar 6. Tampilan Program

9. Analisa

Dari Gambar 4, dapat dijelaskan alur program *flowchart* yaitu program akan melakukan proses validasi terhadap image yang diunggah. Syaratnya adalah file harus berupa gambar atau JPEG. Jika pengguna ingin membuat file stegano saja atau hanya menyisipkan pesan, maka cukup mengisikan pesan yang akan disisipkan pada *text box* yang disediakan. Akan tetapi jika pengguna ingin membuat file yang bersifat rahasia dan hanya bisa dibuka oleh pihak yang berkepentingan, maka pengguna dapt mengisikan *key* atau "*encrypt/decrypt data*" pada *text box* yang sudah disediakan. Tombol submit akan menyimpan hasil dari file yang sudah kita sisipkan pesan.

Dari flowchart Gambar 5, dapat dijelaskan alur program untuk membuka pesan atau teks yang disisipkan pada gambar yang sudah kita lakukan proses stegano. Prosesnya hampir sama dengan proses embedding, yaitu upload file gambar yang akan dibuka isi pesannya. Jika file yang disimpan adalah rahasia, maka menggunakan *key* untuk membuka isi dari pesan tersebut.

10. Kesimpulan

Dari hasil percobaan sistem yang telah dibuat maka dapat disimpulkan bahwa file yang mengalami proses *embedding* atau proses penyisipan pesan, file tidak mengalami banyak perubahan dengan kata lain gambar yang dihasilkan masih sama dengan file aslinya, hanya berbeda pada *size* atau ukurannya.

Dengan menggunakan teknik steganografi dan kriptografi memungkinkan untuk validasi keabsahan suatu sertifikat yang diterbitkan secara online, karena setiap pihak bisa mengecek keaslian dari sertifikat tersebut.

Daftar Pustaka

[1] Sasongko, Jati. "*Pengamanan Data Informasi menggunakan Kriptografi Klasik*". Fakultas Teknologi Informasi. Universitas Stikubank Semarang. 2005

[2] Aditya Yogie, Pratama Andhika dan Nurlifa Alfian. *"Studi Pustaka Untuk Steganografi Dengan Beberapa Metode*". Fakultas Teknologi Industri. Universitas Islam Indonesia, 2010

[3] David, Murtado A. dan Kasma Utin. *"Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media*

Online". Program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak, 2012

[4] Westfeld Andreas. "*Steganalysis in the Presence of Weak Cryptography and Encoding*". Technische University¨at Dresden Institute for System Architecture, Germany, 2006

[5] Utami Ema. *"Pendekatan Metode Least BIT Modification Untuk Merancang Aplikasi Steganography Pada File Audio Digital Tidak Terkompresi"*. STMIK AMIKOM Yogyakarta, 2009