(P) ISSN 2442-4512
(O) ISSN 2503-3832

TEKNIK STEGANOGRAFI DAN ENKRIPSI DOKUMEN GUNA MENJAMIN KEAMANAN DAN INTEGRITAS INFORMASI DALAM LINGKUP ORGANISASI (STUDI KASUS PADA PT SAPTAWARA TEKNOLOGI INDONESIA)

Sandy Martsanto[1)], Wildan Jazuli[2)]

[1)2)]Program Studi Magister Ilmu Komputer
Pascasarjana
Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan 12260 Indonesia
sandy.martsanto@gmail.com[1)], jazuli.wildan@gmail.com[2)]

ABSTRAK

Integritas informasi sangat dibutuhkan dewasa ini, berbagai macam penyalahgunaan wewenang ditengarai sebagai pemicu utama terjadinya pelanggaran hukum, konsep ini memungkinkan pengguna untuk mengirimkan dokumen yang terjamin keaslian informasinya kepada pengguna lain tanpa harus khawatir terjadinya penyalahgunaan atau manipulasi informasi yang dikirimkan. Media yang digunakan adalah berupa gambar digital. Teknik ini dibangun dengan menggunakan bahasa pemrograman *PHP*. Metode *Least Significant Bit Insertion (LSB)* merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai *covertext*. Pada susunan bit di dalam sebuah *byte (1 byte = 8 bit)*, ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (least significant bit atau *LSB*). Metode *Vigenere Chiper* digunakan untuk melakukan proses kriptografi pada teknik ini. *Vigenere Chiper* merupakan metode enkripsi klasik yang menggunakan bujursangkar *vigenere* sebagai kunci.

Kata Kunci: *steganografi, PHP, enkripsi, integritas, LSB, Vigenere Cipher*

ABSTRACT

Integrity of information is needed today, various kinds of abuse of authority is considered as a major trigger for violations of the law, this concept allows users to send a document that guaranteed the authenticity of the information to another user without having to worry about the misuse or manipulation of information that is sent. The media used is in the form of digital images. This technique is built using PHP programming language. Least Significant Bit (LSB) is a method of steganography most simple and easy to implement. This method uses a digital image as covertext. In the arrangement of bits in a byte (1 byte = 8 bits), there is the most significant bit (most significant bit or MSB) and the least significant bit (least significant bit or LSB). Vigenere Chiper method used to perform cryptographic processes on this technique. Vigenere Chiper is a classic encryption method that uses a square vigenere as a key.

Keywords: *steganography, PHP, encryption, integrity, LSB, Vigenere Chiper*

(P) ISSN 2442-4512
(O) ISSN 2503-3832

1. PENDAHULUAN

Latar Belakang

Seiring berkembang pesatnya teknologi dewasa ini seakan memudahkan segala hal dapat tercapai dengan cepat, era digitalisasi media semakin marak hingga komunikasi tak lagi dipisahkan oleh jarak dan waktu. Hal tersebut melahirkan implikasi negatif yang rentan terhadap manipulasi digital dan menurunnya integritas suatu data ataupun informasi, dalam kehidupan era sekarang ini dapat terlihat dengan banyaknya kasus penyalahgunaan wewenang jabatan yang ditengarai sebagai akibat adanya informasi yang salah ataupun di manipulasi, seorang pejabat tertangkap dengan tuduhan dokumen yang ditandatangani adalah delik aduan sebagai penyebab kerugian negara, namun disisi lain pejabat tersebut menyangkalnya dengan menunjukkan dokumen yang asli. Hal inilah yang menjadi latar belakang penulis untuk membangun teknik steganografi dan enkripsi dokumen untuk menjamin keamanan dan integritas dokumen dalam suatu organisasi.

Salah satu program pemerintah saat ini yaitu meminimalisir penggunaan kertas, selain bertujuan untuk mengurangi biaya dan emisi karbon, program ini juga bertujuan untuk beralih daya dalam menyajikan informasi dari bentuk *paper* (kertas) menjadi *paperless* (tanpa kertas), komunikasi antar satuan kerja maupun lintas lembaga diarahkan untuk menggunakan solusi internet sebagai contoh dalam berkirim surat sebaiknya melalui fasilitas *email (electronic mail),* kerentanan terhadap integritas data atau informasi sangat tinggi, jika tidak ada *awarness* (kesadaran) terhadap upaya menjaga keamanan data dan informasi bagi penggunanya, manipulasi data dan perusakan data menjadi hal yang harus diwaspadai dalam pertukaran informasi tersebut.

Menjaga integritas data dan informasi tak lepas dari metode keamanan terhadap objek data dan informasi tersebut. Terdapat beberapa metode untuk menjaga keamanan data dan informasi diantaranya dengan kriptografi dan steganografi.

Identifikasi Masalah

Berdasarkan latar belakang permasalahan diatas, permasalahan dapat diidentifikasi antara lain:

a. Bagaimana pemanfaatan metode steganografi untuk menjaga integritas dan keamanan data dan informasi?
b. Bagaimana pemanfaatan metode kriptografi untuk menjaga integritas dan keamanan data dan informasi?

Lingkup

Adapun yang menjadi ruang lingkup masalah tersebut adalah sebagai berikut:

a. Penelitian difokuskan pada pembuatan aplikasi untuk melakukan *encoding* dan menampilkan pesan atau kunci terhadap suatu dokumen dalam bentuk citra dan selanjutnya proses *decode* untuk membuktikan keaslian *file* atau dokumen yang dimaksud.
b. Penelitian difokuskan pada pembuatan aplikasi untuk melakukan enkripsi dan dekripsi suatu dokumen dalam bentuk citra.
c. Penggabungan kedua metode steganografi dan enkripsi dalam satu sistem aplikasi.

Tujuan

Tujuan dari penelitian ini adalah:

a. Memberikan pemahaman tentang arti pentingnya keamanan dan integritas data dan informasi
b. Memberikan kesadaran terhadap segala bentuk penyalahgunaan data dan informasi
c. Memberikan solusi terhadap kebutuhan keamanan dan menjamin integritas data dan informasi pada suatu organisasi.

2. LANDASAN TEORI

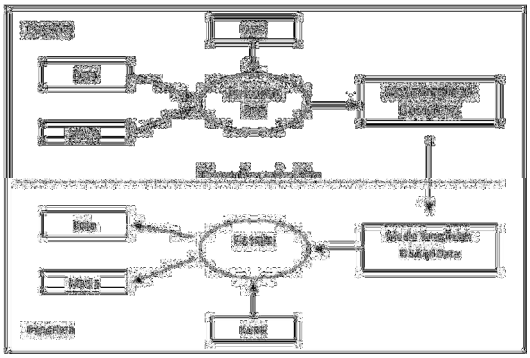
Tinjauan Pustaka

Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia didalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui.[1]

Steganografi membutuhkan dua poperti yaitu, media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode program atau pesan lain.

Konsep steganografi dapat dilihat dari diagram berikut



Gambar 1. Konsep dasar Steganografi

Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Ini berbeda dengan kriptografi dimana *ciphertext* menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia.

Beberapa metode umum yang digunakan untuk menyembunyikan pesan ataupun data dalam sebuah

(P) ISSN 2442-4512
(O) ISSN 2503-3832

citra dalam steganografi, metode tersebut diantaranya:

a. *Least Significant Bit Insertion (LSB)*
   Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. Pada susunan *bit* di dalam sebuah *byte* (1 byte = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan *bit* yang paling kurang berarti *(least significant bit atau LSB)*.
b. *Algorithms and Transformation*
   Algoritma compression adalah metode steganografi dengan menyembunyikan data dalam fungsi matematika. Dua fungsi tersebut adalah *Discrete Cosine Transformation (DCT)* dan *Wavelet Transformation*. Fungsi *DCT* dan *Wavelet* yaitu mentransformasi data dari satu tempat (domain) ke tempat (domain) yang lain. Fungsi *DCT* yaitu mentransformasi data dari tempat *spatial (spatial domain)* ke tempat frekuensi *(frequency domain)*.[2]
c. *Redundant Pattern Encoding*
   Redundant Pattern Encoding adalah menggambar pesan kecil pada kebanyakan gambar. Keuntungan dari metode ini adalah dapat bertahan dari *cropping* (kegagalan). Kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar.[2]
d. *Spread Spectrum Method*
   Spread Spectrum steganografi terpencar-pencar sebagai pesan yang diacak *(encrypted)* melalui gambar (tidak seperti dalam *LSB*). Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image* (gambar).[2]

Adapun jenis citra yang dapat disisipi pesan dalam steganografi adalah sebagai berikut:

a. *JPG / JPEG (Joint Photographic Experts Assemble)*
   JPG adalah jenis data yang dikembangkan oleh *Joint Photographic Experts Assemble (JPEG)* yang dijadikan standar untuk para fotografer profesional. [3]
b. *GIF (Graphics Interchange Format) GIF*
   sama seperti *JPG*, adalah format gambar yang sudah cukup lama digunakan dan salah satu yang umum dipakai di internet. *GIF* adalah kepanjangan *dari Graphics Interchange Format. GIF* secara alami adalah gambar dengan 8-*bit* warna, berarti mereka dibatasi oleh palet sebanyak 256 jenis warna, yang dapat dipilih dari model RGB dan disimpan ke *Color Look Up Tablet (CLUT)*, atau sederhananya *"Color Table"*. Mereka itu sejatinya adalah palet warna standar, seperti palet *"Web Safe"*.Selain bisa transparansi, *GIF* juga mendukung animasi gambar yang membatasi tiap form nya pada 256 warna standar. Dan karena sifatnya yang tidak pecah-pecah, *GIF* bisa digunakan untuk menjaga baris dalam tipografi tetap rapi, dan juga bentuk-bentuk geometri.[3]
c. *PNG (Portable Network Graphic)*
   PNG adalah kepanjangan *dari Portable Network Graphics*. Dikembangkan sebagai alternatif lain untuk *GIF*, yang menggunakan paten dari *LZW–* algoritma kompresi. *PNG* adalah format gambar yang sangat baik untuk grafis internet, karena mendukung transparansi didalam perambah *(browser)* dan memiliki keindahan tersendiri yang tidak bisa diberikan *GIF* atau bahkan *JPG*. Kelebihan *file PNG* adalah adanya warna transparan dan alpha. Warna *alpha* memungkinkan sebuah gambar transparan, tetapi gambar tersebut masih dapat dilihat mata seperti samar-samar atau bening.[3]
d. *BMP (Bitmap)*
   Bitmap adalah representasi dari citra grafis yang terdiri dari susunan titik *(pixel)* yang tersimpan di memori komputer. Nilai setiap titik diawali oleh satu *bit* data (untuk gambar hitam putih) atau lebih (untuk gambar berwarna). Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam gambar ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom (contoh 1024×768).[3]
e. *TIFF (Tagged Image Format File)*
   TIFF merupakan format gambar terbaik dengan pengertian bahwa semua data dan informasi (data *RGB*, data *CMYK*, dan lainnya) yang berkaitan dengan koreksi atau manipulasi terhadap gambar tersebut tidak hilang. Format *TIFF* biasa digunakan untuk kebutuhan pencetakan dengan kualitas gambar yang sangat tinggi sehingga ukuran berkas untuk format ini biasanya sangat besar, karena dalam *file* ini gambar tidak dikompresi. Format ini mampu menyimpan gambar dengan kualitas hingga 32 *bit*. Format berkas *TIFF* juga dapat digunakan untuk keperluan pertukaran antar *platform (PC, Macintosh, dan Silicom Graphic)*. Sebuah pesan steganografi *(plaintext)*, biasanya pertama-tama 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

(P) ISSN 2442-4512
(O) ISSN 2503-3832

mengetahui teknik yang digunakan) dapat membuka pesan dan mendekripsikannya.[3]

Kriptografi

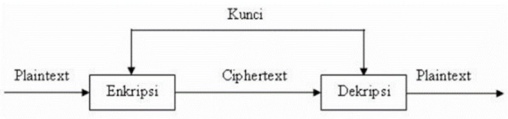
Kriptografi *(cryptography)* berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.[4]. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.

Proses utama pada kriptografi antara lain:

a. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim, diubah menjadi bentuk yang hampir tidak dapat dikenali sebagai informasi pada awalnya dengan menggunakan algoritma tertentu.
b. Deskripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk yang disamarkan menjadi informasi awal.

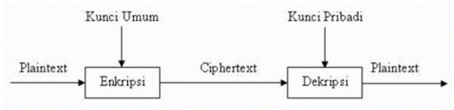
Teknik kriptografi untuk enkripsi data ada dua macam, antara lain:

1. *Kriptografi Simetris*
   Algoritma simetris atau sering disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran *(Stream Ciphers)* dan algoritma blok *(Block Ciphers)*. Dimana pada algoritma aliran, proses penyandiannya akan beriorientasi pada satu *bit/byte* data. Sedangkan pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan *bit/byte* data (per blok). Adapun contoh algoritma kunci simetris adalah *DES (Data Encryption Standard), blowfish, twofish, MARS, IDEA, 3DES* (*DES* diaplikasikan 2 kali), *AES(Advanced Encryption Standard)* yang bernama asli Rijndael.



Gambar 2. Proses enkripsi/deskripsi algoritma simetris

2. *Kriptografi Asimetris*
   Kriptografi asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan deskripsi. Dimana kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik *(public key)*, sedangkan kunci deskripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi *(private key)*. Oleh karena itu, kriptografi ini dikenal pula dengan nama kriptografi kunci publik *(public key cryptography)*. Adapun contoh algoritma yang menggunakan kunci asimetris adalah *RSA (Riverst Shamir Adleman)* dan *ECC (Elliptic Curve Cryptography)*. Adapun pada kriptografi asimetris, dimana setiap pelaku sistem informasi akan memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi, dimana kunci publik di distribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri. Artinya bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendeskripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut.



Gambar 3. Proses enkripsi/deskripsi algoritma asimetris

Vigenere Chiper

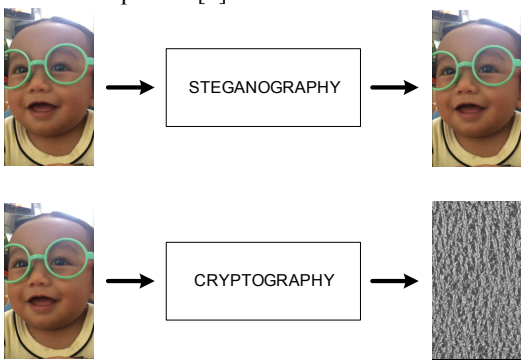
Metode *Vigenere Chiper* adalah suatu metode yang mengubah pesan dengan menggunakan kombinasi 26 huruf alfabet. Algoritma *Vigenere Cipher* memiliki beberapa kelemahan, diantaranya hanya menampung 26 huruf alfabet dalam bentuk huruf kecil, sedangkan tanda baca lain tidak dapat terbaca. Untuk itu perlu dilakukan suatu pengevaluasian yaitu dengan memperluas jangkauan 26 huruf alfabet tersebut menjadi 256 karakter *ASCII*.[5]

Perbedaan Steganografi dengan Kriptografi

Steganografi berbeda dengan kriptografi, letak perbedaannya adalah pada hasil keluarannya. 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 menggunakan komputer atau perangkat pengolah digital lainnya

(P) ISSN 2442-4512
(O) ISSN 2503-3832

dapat dengan jelas dibedakan antara sebelum proses dan setelah proses. [6]



Gambar 4. Ilustrasi perbedaan antara steganografi dan kriptografi

3. METODE PENELITIAN

Penggunaan metode *Least Significant Bit Insertion (LSB)* untuk diaplikasikan dalam proses *encoding* yang kemudian digabungkan dengan metode *vigenere chiper* untuk proses enkripsi.

Data diambil dari beberapa sampel dokumen yang memungkinkan dimiliki oleh beberapa pihak, baik staf atau karyawan perusahaan ataupun pihak lain yang berkepentingan. Seluruh dokumen fisik akan di identifikasi keasliannya, dokumen tersebut kemudian di pindai *(scan)* menggunakan alat pemindai, yang kemudian hasilnya nanti akan berupa gambar atau citra berkestensi file *.jpg*. Citra tersebut selanjutnya akan dimasukkan ke dalam database sebagai arsip digital.

Ujicoba sistem dilakukan dengan 5 buah dokumen digital, dimana setiap dokumen tersebut akan dibagikan kepada setiap staf atau karyawan, dokumen digital dengan nama *Dok5.jpg* sengaja dibuat sedemikian rupa agar membutuhkan perubahan gambar dari segi kecerahannya *(brightness)* yang nantinya memicu staf atau karyawan untuk merubah gambarnya. Dokumen digital dengan ekstensi *.jpg* yang melalui proses *encoding* akan menghasilkan ekstensi .png.

No	Nama Dokumen	Ukuran Asli	Ukuran setelah Encode	Key/ Kunci
1	Dok1.jpg	211 KB	401 KB	KTRJY
2	Dok2.jpg	118 KB	375 KB	KTRJY
3	Dok3.jpg	560 KB	2,42 MB	KTRJY
4	Dok4.jpg	311 KB	0,98 MB	KTRJY
5	Dok5.jpg	121 KB	192 KB	KTRJY

Tabel 1. Data Sampel Dokumen

4. HASIL PENELITIAN

Desain Sistem

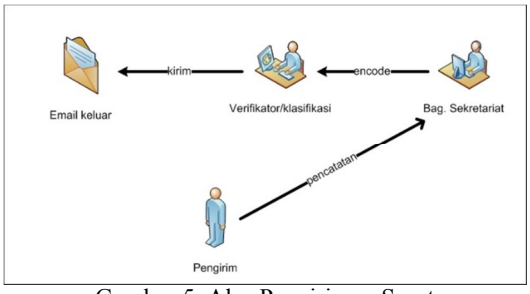
Sistem dibangun berdasarkan kebutuhan pengguna untuk melakukan *encoding* dan *decoding* dokumen yang memiliki tingkat urgensi tinggi seperti:

a. Surat Keluar dalam hal penggunaan Uang Negara
b. Perjanjian dengan pihak lain
c. Pernyataan diatas Materai
d. Kartu Tanda Penduduk
e. Dan lain sebagainya yang dianggap penting

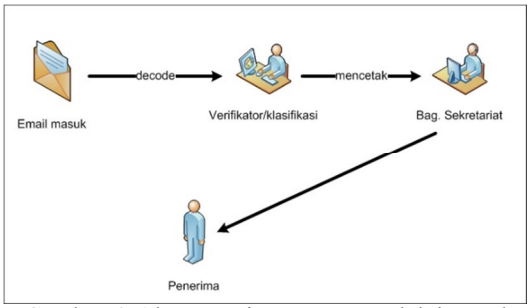
Sebelum melakukan *encoding* seluruh bentuk dokumen kertas yang sudah diverifikasi oleh sekretariat, akan di pindai *(scan)* melalui alat bantu *scanner*, setelah itu proses *encoding* dilakukan.

Berbeda dengan proses *decoding*, dimana surat masuk yang diterima melalui *email* (surat elektronik) dapat langsung diverifikasi *(decode)* untuk mengetahui keaslian dan keabsahannya.

Ada beberapa standar internal yang bersifat rahasia perihal isi dari pesan atau kunci yang akan ditampilkan untuk membuktikan keaslian dan keabsahan dokumen baik yang diterima maupun dikirim.



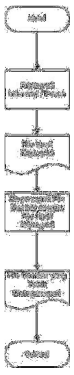
Gambar 5. Alur Pengiriman Surat



Gambar 6. Alur Penerimaan surat melalui *email*

Flowchart Aplikasi

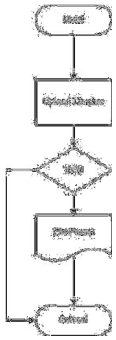
Berikut *Flowchart* proses *encode* dari aplikasi yang akan dibangun



(P) ISSN 2442-4512
(O) ISSN 2503-3832

Gambar 7. *Flowchart* proses *encode*

Berikut *Flowchart* proses *decode* dari aplikasi yang akan dibangun



Gambar 8. *Flowchart* proses *decode*

Kebutuhan Sistem

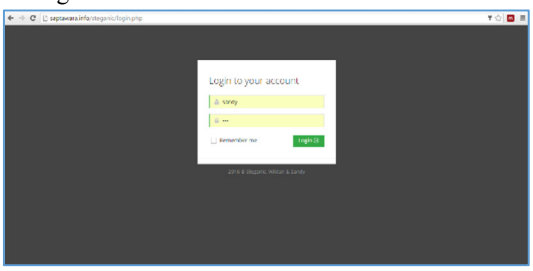
Sistem dibangun dengan menggunakan bahasa pemrograman *PHP,* hal ini dimaksudnya untuk menjadikan aplikasi bisa digunakan oleh siapa saja sesuai kebutuhan, tersentralisasi, fleksibel dan lebih reliabel.

Adapun kebutuhan perangkat keras diantaranya:

a. *Processor* minimal setara *Pentium IV* atau lebih
b. *Memory* minimal setara 1*GB* atau lebih
c. *Space Harddisk* minimal setara 10*GB* atau lebih
d. Monitor
e. Printer
f. Scanner

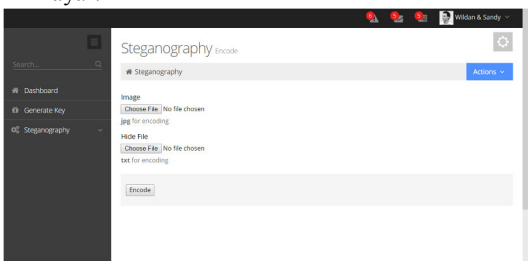
Antarmuka

Berikut desain antarmuka dari aplikasi yang akan dibangun



Gambar 9. Antarmuka *form Login*

Masukkan *Username* dan *Password* kamudian tekan tombol *"Login"*, setelah berhasil masuk, sistem akan menampilkan pilihan menu disamping kiri layar.

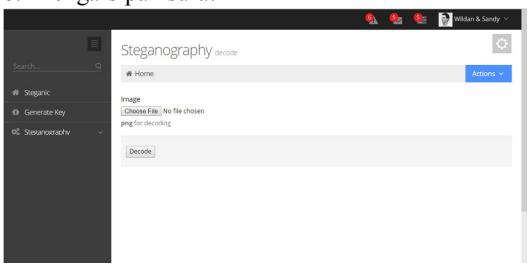


Gambar 10. Antarmuka halaman *encode*

User akan memilih beberapa menu pilihan sesuai kebutuhan.

Menu *Dashboard* berisi *file* apa saja yang telah di-encoding dan yang di-*decoding*, hal ini dimaksudkan untuk melihat *history* (sejarah) penggunaan aplikasi, juga beberapa hal yang dimaksudkan diantaranya:

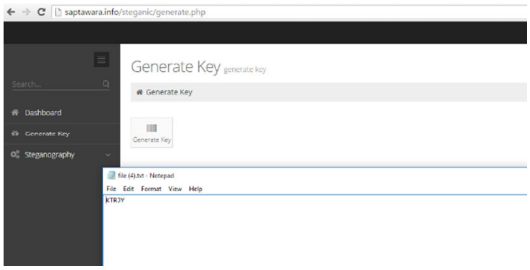
a. Proses *Audit Trail* yaitu proses melakukan audit yang berkenaan dengan kebutuhan investigasi atas sumberdaya yang digunakan
b. Pengarsipan surat



Gambar 11. Antarmuka halaman *decode*

Pilih menu *"Steganography"* kemudian pilih *"decode"* untuk melakukan proses *decoding*, selanjutnya pilih *file* dokumen yang berekstensi *.png* yang sebelumnya diterima. Lakukan proses *decode* dengan menekan tombol *"Decode"*.

Proses *decode* akan mengunduh *file .txt* pada gambar yang dimaksud, dan menampilkan isi kunci atau *key* yang telah disisipkan sebelumnya pada proses *encode*, jika hasilnya sama dengan *key* atau kunci yang disisipkan pada proses *encode*, maka hal itu membuktikan bahwa *file* atau dokumen digital yang dimaksud adalah asli identik tanpa ada perubahan apapun.



Gambar 12. *Generate Key*

Pilih menu *"Generate Key"* untuk mengunduh *file .txt* yang berisi pesan atau kunci hasil dari proses enkripsi, dan kemudian akan digabungkan pada proses *encode*.

Implementasi

Implementasi sistem adalah tahap penerapan sistem yang akan dilakukan jika sistem disetujui termasuk program yang telah dibuat pada tahap perancangan sistem agar siap untuk dioperasikan.

Implementasi aplikasi yang diberi nama Steganic berbasis web ini menggunakan bahasa pemrograman *PHP*. Implementasi dan pengujian sepenuhnya hanya dilakukan pada perangkat keras

(P) ISSN 2442-4512
(O) ISSN 2503-3832

PC (Personal Computer) dengan sistem operasi *Microsoft Windows 10*.

Kebutuhan perangkat lunak diantaranya:

a. *Microsoft Windows 10* sebagai sistem operasi
b. XAMPP sebagai *Webserver*

Pengujian

Pengujian dilakukan dengan melakukan *decode* dari 5 sampel dokumen digital, jika pada setiap hasil decode menampilkan *key* atau kunci yang sama pada saat proses *encode*, maka hal ini membuktikan bahwa *file* atau dokumen digital tersebut tidak melalui proses perubahan atau identik.

Hasil pengujian teknik ini terhadap 5 sampel dokumen tersebut dapat dilihat dalam tabel berikut.

No	Nama *File*	Ukuran yang diterima	*Key* yang dihasilkan
1	Dok1.png	401 KB	KTRJY (asli)
2	Dok2.png	375 KB	KTRJY (asli)
3	Dok3.png	2,42 MB	KTRJY (asli)
4	Dok4.png	0,98 MB	KTRJY (asli)
5	Dok5.png	193 KB	Error (dirubah)

Tabel 2. Hasil pengujian

Dari hasil pengujian tersebut diketahui bahwa *file* atau dokumen digital dengan nama *Dok5.png* telah melalui perubahan, hal itu dapat diketahui dari perbedaan ukuran file atau dokumen yang awalnya 192*KB* menjadi 193*KB* (kenaikan 1*KB*), dan hasil pengujian *key* atau kunci tidak berhasil *(error)*.

5. PENUTUP

Kesimpulan

a. Aplikasi steganografi ini, befungsi untuk mengetahui keaslian informasi gambar yang diterima.
b. Dengan aplikasi steganografi ini, pengguna dapat mengamankan data sehingga tidak dapat dipalsukan.
c. Adanya penambahan ukuran setiap *file* atau dokumen setelah proses *encode*.
d. Metode *Vigenere Chiper* memiliki kelemahan hanya mampu menampung 26 huruf alfabet, yang mungkin lebih mudah untuk dipecahkan.

Saran

a. Steganografi dan kriptografi dapat diintegrasikan menjadi satu kesatuan aplikasi system yang sebaiknya diimplementasikan disetiap lingkungan organisasi untuk menjagi integritas data dan informasi.
b. Peningkatan keamanan dalam penyembunyian pesan sebagai identitas setiap *file* atau dokumen dapat dikembangkan dengan metode steganografi dan kriptografi lainnya, sehingga dapat menyisipkan lebih banyak pesan, key atau kunci tertentu tanpa mempengaruhi citra penampungnya secara signifikan.

DAFTAR PUSTAKA

[1] R. Munir, “Kriptografi,” no. Informatika Bandung. Informatika Bandung, 2006.
[2] Wikipedia.org, “Steganografi.” p. https://id.wikipedia.org/wiki/Steganografi– 14 Mei, 2016.
[3] G. M. Arini and T. I. Widyawan, “Pengamanan Pesan Steganografi dengan Metode LSB Berlapis Enkripsi dalam PHP,” *Pengamanan Pesan Steganografi dengan Metod. LSB Berlapis Enkripsi dalam PHP*, p. 11.
[4] A. Menezes, V. Oorschot, and S. Vanstone, “Handbook of Applied Cryptography,” *Handb. Appl. Cryptogr.*, no. CRC Press, 1997.
[5] E. K. Nurnawati, “Analisis Kriptografi Menggunakan Algoritma Vigenere Cipher Dengan Mode Operasi Cipher Block Chaining (CBC),” pp. 266–272, 2008.
[6] H. Suhono, Supangkat, “Watermarking Sebagai Teknik Penyembunyian Hak Cipta Pada Data Digital,” no. Jurnal Departemen Teknik Elektro, Institut Teknologi Bandung., 2000.