STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT(LSB) DENGAN KOMBINASI ALGORITMA KRIPTOGRAFI BLOCKING, PERMUTASI, PEMAMPATAN DAN *VIGENERE*

Avin Kusuma Putra*, Suwitno†, dan Yosep Lazuardi‡
Fakultas Teknologi Informasi
Universitas Budi Luhur
Jakarta, Indonesia
Email: *avin.putra12@gmail.com, †suwit.ang1305@gmail.com, ‡yoseplazuardi@yahoo.com

Abstract—Security and confidentiality are important aspects needed in the exchange of messages through the network media / internet. Cryptography and steganography techniques can be used to provide security protection to the secret message. Developing multiple cryptographic techniques with classic cryptography algorithm combinations blocking, permutation, compression and *vigenre* are integrated into the steganography using LSB (Least Significant Bit) methods is expected to protect confidential messages. This study aims to combine classical cryptography blocking, permutation, compression and *vigenre* integrated with steganography methods, to provide double protection to the secret message within an image/ digital image. Results from this study is an application named "CryptoStego" which has succeeded in combining cryptography and steganography."CryptoStego" application can be running on a Windows-based operating system using Microsoft Excel 2013 application, and can only hide text message into a bitmap or jpeg format images. Therefore it is necessary for the development of further applications can hide a message into a format other than a bitmap and jpeg images, and can hide text message into the media in addition to images such as audio and video, and can be used globally on all operating systems.

Index Terms—Data Security, Cryptography, Steganography, Least Significant Bit, *Vigenre.*

1 PENDAHULUAN

Keamanan suatu sistem informasi pada era digital ini makin penting peranannya dalam berbagai aspek kehidupan, terutama untuk informasi yang memiiki nilai lebih dibanding dengan informasi yang lain, misalnya informasi yang berkaitan dengan aspek aspek keputusan bisnis, kemanan Negara, ataupun kepentingan umum, tentunya informasi informasi tersebut diminati oleh berbabagi pihak. Oleh karena itu pengamanan informasi dalam hal ini adalah steganografi, semakin dibutuhkan guna memberikan rasa aman dalam proses penyampaian informasi. Steganografi sendiri merupakan cara untuk menyembunyikan rahasia didalam suatu informasi lain yang tampak tidak bermakna, kecuali bagi orang yang mengerti kuncinya. Teknik steganografi menggunakan dua media yang berbeda secara bersamaan, dimana salah satu berfungsi sebagai media yang berisikan informasi informasi rahasia. 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 informatika komputer, ada 2 istilah teknik keamanan data yang sangat dikenal yaitu kriptografi dan steganografi. Kriptografi dan steganografi 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)[6], 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.

2 STUDI PUSTAKA

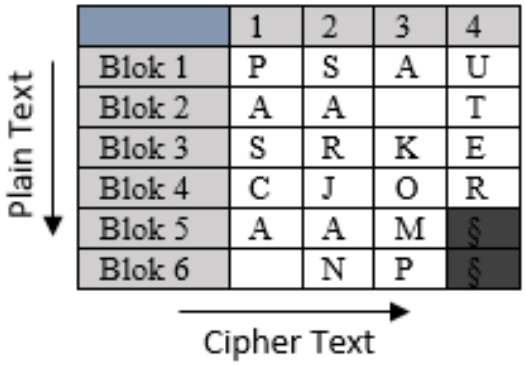
2.1 Algoritma Blocking

menjadi beberapa blok yang terdiri dari beberapa karakter, kemudian di enkripsikan secara independen. Caranya : Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya. Jumlah blok yang dihasilkan merupakan hasil pembagian keatas (ceiling) dari jumlah karakter plaintext dengan jumlah karakter setiap blok. contoh: Plaintext: PASCA SARJANA KOMPUTER Setiap blok terdiri dari 4 karakter Maka dilakukan perhitungan jumlah blok sebagai berikut:

$$N_Blok = NCharPlaintext/CharPerBlok$$

$$Blok = 22/4 = 5.5$$

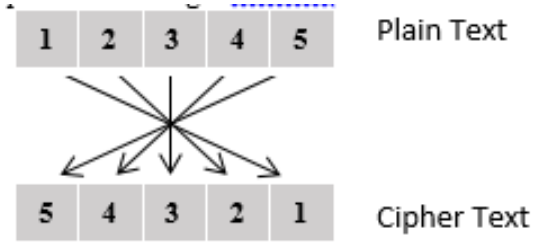
=¿ 6(selalu dibulatkan ke atas) Dari hasil perhitungan tersebut diatas terdapat 6 blok (dengan asumsi setiap blok 4 karakter)
Untuk membedakan dengan spasi, biasanya setiap ruang kosong yang tesisa disetiap blok paling akhir akan ditambahkan simbol yang sangat jarang atau tidak pernah digunakan dan simbol yang digunakan harus sama untuk setiap ruang kosong paling akhir dari setiap blok. Simbol khusus ini akan dihilangkan dari plaintext setiap ada proses dekripsi dengan tujuan untuk menghindari kesalahan yang terjadi. Sehingga dapat digambarkan sebagai berikut:



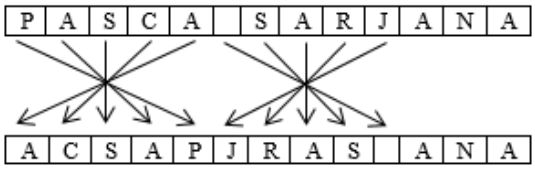
Gambar. 1. contoh Algoritma Blocking

2.2 Algoritma Permutasi

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama. Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 5 karakter, dengan aturan sebagai berikut:



Gambar. 2. contoh Algoritma Permutasi



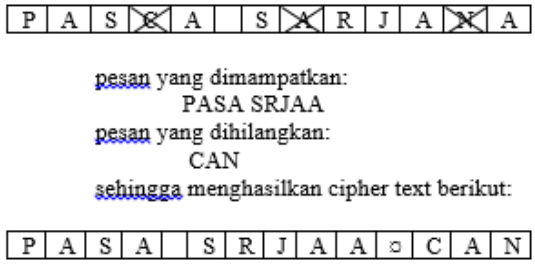
Gambar. 3. contoh proses Permutasi

Plain Text: PASCA SARJANA

Cipher Text: ACSAPJRAS ANA

2.3 Algoritma Pemampatan (Compaction)

Teknik algoritma enkripsi ini dengan mengurangi panjang pesan atau bloknya untuk menyembunyikan pesan, misakan menghilangkan setiap karakter ke-empat secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali dan diusulkan sebagai lampiran dari pesan utama, dengan diawali oleh suatu karakter khusus. Proses yang terjadi adalah berikut:



Gambar. 4. contoh proses Permutasi

2.4 Algoritma Vigenere Cipher

Kode vignere termasuk kode abjad-majemuk (polyalphabetic substitution cipher). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vignere pada abad 16, tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarkannya untuk pertama kali pada tahun 1533 seperti ditulis di dalam buku La Cifra del Sig. Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode vignere. Vignere merupakan pemicu perang sipil di Amerika dan kode vignere digunakan oleh Tentara Konfederasi (Confederate Army) pada perang sipil Amerika (American Civil War). Kode vignere berhasil

dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. (Ariyus, 2008).
Algoritma enkripsi jenis ini sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan ciphertext bisa dilakukan menggunakan substitusi angka maupun bujursangkar vignere. Teknik susbtitusi vignere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.
Contoh:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar. 5. Contoh Tabel Substitusi Algoritma Kriptografi Vigenere Cipher

Plaintext: PLAINTEXT
Kunci : CIPHER

Plain	15	11	0	8	13	19	4	23	19
Kunci	2	8	15	7	4	17	2	8	15
Hasil	17	19	15	15	17	10	6	5	8
Ciphertext	R	T	P	P	R	K	G	F	I

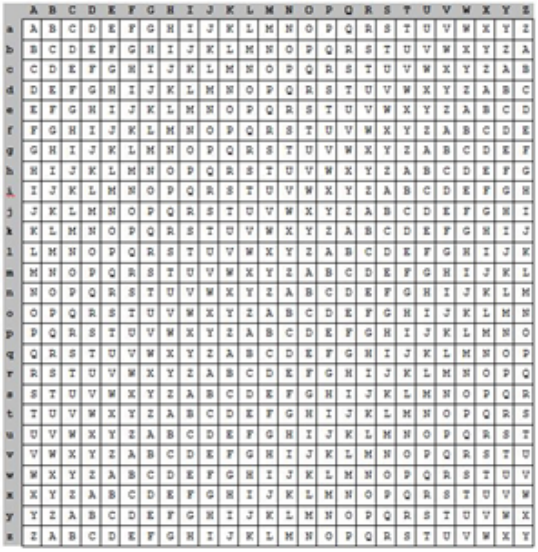
Gambar. 6. Contoh Tabel Kriptografi dengan Algoritma Vigenere Cipher

Dengan metode pertukaran angka dengan huruf di atas, diperoleh bahwa teks asli (PLAINTEXT) memiliki kode angka (15,11, 0, 8, 13, 19, 4, 23, 19), sedangkan kode angka untuk teks kunci (CIPHER) yaitu (2, 8, 15, 7, 4, 17). Setelah dilakukan perhitungan, maka dihasilkan kode angka ciphertext (17, 19, 15, 15, 17, 10, 6, 5, 8). Jika diterjemahkan kembali menjadi huruf sesuai urutan awal, maka menjadi huruf RTPPRKGFI. Sedangkan metode lain untuk melakukan proses enkripsi dengan metode vignere cipher yaitu menggunakan tabula recta (disebut juga bujursangkar vignere).

Variasi-variasi vignere cipher pada dasarnya perbedaannya terletak pada cara membentuk tabel atau cara menghasilkan kuncinya, sedangkan enkripsi dan dekripsi tidak berbeda dengan vignere cipher standar.

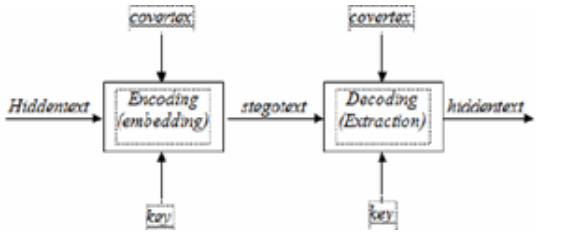
2.5 Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain, sehingga keberadaan pesan rahasia tersebut tidak dapat diketahuai. Steganografi berasal dari bahasa Yunani, yaitu steganos yang artinya tulisan tersembunyi. Steganografi dapat dianggap sebagai

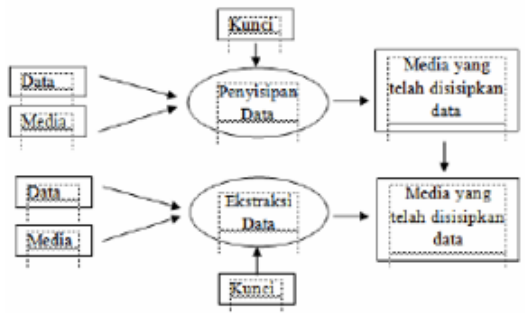


Gambar. 7. Contoh Tabula Recta Algoritma Kriptografi Vigenere Cipher

kelanjutan dari kriptografi dan mempunyai hubungan yang erat, namun pada prakteknya steganografi dan kriptografi adalah dua hal yang berbeda. Dalam prakteknya kebanyakan teknik steganografi diselesaikan dengan melakukan perubahan tipis terhadap data digital yang disisipi pesan rahasia yang isinya tidak akan menarik perhatian dari penyerang atau orang ketiga. Teknik steganografi ini sudah sangat banyak digunakan pada steganografi komputer. Format file digital yang dapat digunakan pada steganografi diantaranya:
1. Format image : bitmap (.bmp), gif, jpg / jpeg, pcx, dll.
2. Format audio : wav, amr, mp3, voc, dll.
3. Format video : avi, mp4, 3gp, flv, dll.
4. Format lain : teks, html, pdf, dll.
Pada masa kini, steganografi banyak dilakukan pada data digital dengan menggunakan medai digital, seperti teks, citra, audio dan video. Steganografi digital ditekankan pada kinerja dan teknik penyisipan pesan agar sedapat mungkin pesan yang disisipkan kedalam medai digital tidak mengubah kualitas media digital tersebut. Steganografi menggunakan dua properti, yaitu wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, audio, teks dan video.[5]. Terdapat beberapa istilah yang berkaitan dengan steganografi:
1. Hiddentext atau embedded message: pesan yang disembunyikan.
2. Covertext atau cover-object: pesan yang digunakan untuk menyembunyikan embedded message.
3. Stegotext atau stego-object: pesan yang sudah berisi embedded message.
4. Stegokey: kunci rahasia.
5. Embedding : proses menyisipkan pesan pada citra sebagai medium penyisipan pesan.
6. Extraction : proses mengambil pesan yang terdapat pada citra atau medium penyisipan.



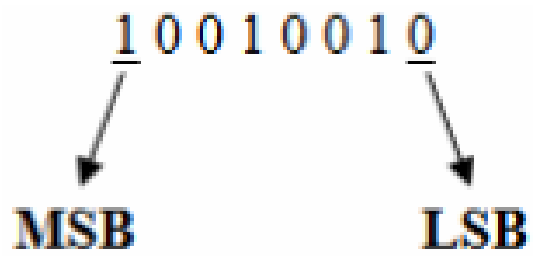
Gambar. 8. Diagram Penyisipan dan Ekstraksi Pesan



Gambar. 9. Diagram Sistem Steganografi

2.6 Metode LSB

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya pada file image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna yaitu merah, hijau, dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Pada proses penyisipan pesan, pesan yang akan disisipkan kedalam citra JPG/JPEG atau Bitmap dalam beberapa tahap. 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).



Gambar. 10. MSB dan LSB

3 Metode Penelitian

Penelitian ini dilakukan berdasarkan permasalahan yang telah di uraikan pada bagian perumusan masalah sebelumnya. Adapun bahan dan tahapan guba penelitian ini adalah:

3.1 Studi pustaka dan literatur

Studi ini dilakukan dengan cara mencari sekaligus mempelajari beberapa literatur dan artikel mengenai kriptografi dan steganografi sebagai acuan dalam pendefinisian, perencanaan, analisa dan pembuatan contoh algoritma atau program untuk mencari solusi yang tepat..

3.2 Instrumen Penelitian

Tujuan dari deskripsi instrumen adalah untuk mengetahui kebutuhan sistem agar mempermudah perancangan. Instrumen ini meliputi kebutuhan perangkat keras dan perangkat lunak sistem. Kebutuhan-kebutuhan di bawah ini merupakan kebutuhan minimal dari sistem :
a) Kebutuhan Perangkat Keras :
Prosesor Core 2 Duo.
Harddisk 100 GB.
Memori 2 GB.
Layar Display 14.
Satu buah mouse dan keyboard standar.
b) Kebutuhan Perangkat Lunak :
Sistem operasi Microsoft Windows 7.
Pada penelitian ini sstem operasi minimal yaitu Microsoft Windows 7, dikarenakan untuk pembuatan sistem menggunakan scrip makro Excel 2013 dan VBA (visual basic application). Software Microsoft Excel 2013
Software pengelola data yang dianjurkan sebagai spesifikasi minimal adalah Microsoft Excel 2013, karena menggunakan script makro yang akan diimplementasikan dengan script vba (visual basic application) dan membaca file .xlsm.

3.3 Pembuatan Program

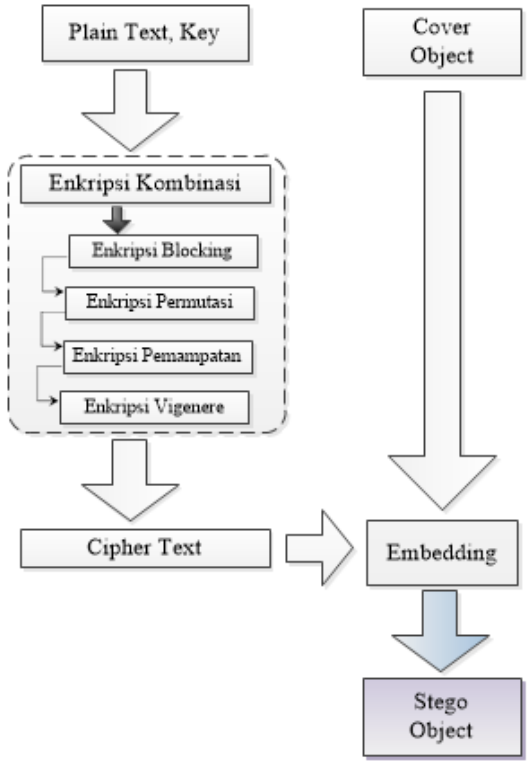
Perancangan dan implementasi sistem yang dilakukan secara eksperimental yaitu bereksperimen membuat program berdasarkan materi dan algoritma yang telah dipelajari.

4 Hasil dan Pembahasan

Algoritma dan proses yang diusulkan telah dijelaskan diatas yaitu penggabungan algoritma kriptografi klasik blocking, permutasi, pemampatan dan vigenere dengan steganografi metode LSB (Least Significant Bit). Dengan menggabungkan algoritma kriptografi klasik kombinasi dan metode LSB dapat meningkatkan keamanan pesan rahasia. Pesan rahasia disandikan dengan menggunakan algoritma kriptografi klasik kombinasi dan disembunyikan pada media file gambar menggunakan metode LSB. Proses utama dari penggabungan algoritma kriptografi klasik kombinasi dan metode LSB adalah proses penyisipan pesan rahasia dan proses membaca pesan rahasia. Proses penyisipan pesan dilakukan dengan menyandikan pesan rahasia atau plaintext menggunakan algoritma enkripsi kriptografi klasik kombinasi menjadi bentuk yang tidak dapat dipahami maknanya atau ciphertext, setelah itu disisipkan pada media atau citra induk yang berupa file gambar menggunakan metode LSB. Hasil dari proses penyisipan adalah file gambar bitmap atau jpg yang disebut dengan stegoimage. Sedangkan proses membaca pesan dilakukan dengan mengambil ciphertext dari stegoimage dan mengubah ciphertext menjadi plaintext dengan menggunakan algoritma dekripsi kriptografi klasik

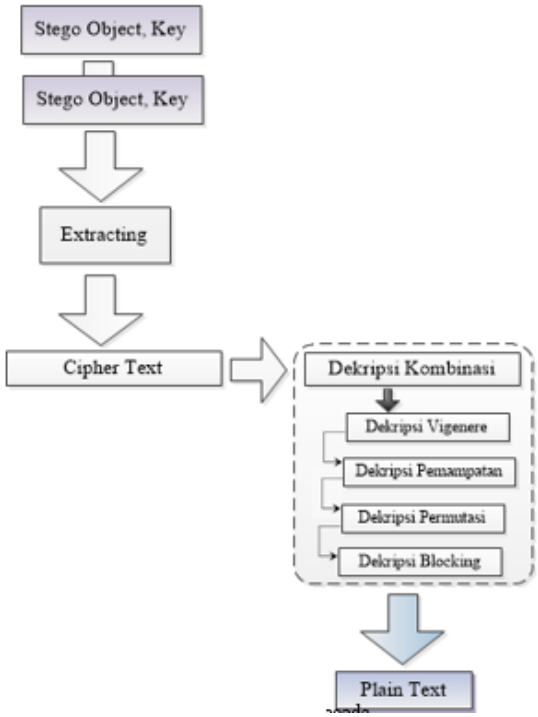
kombinasi.

Gambar 11 merupakan skema dari proses penyisipan pesan, proses ini dilakukan oleh orang yang akan mengirim pesan rahasia. Plaintext berupa pesan teks dienkripsi menjadi ciphertext dengan menggunakan algoritma enkripsi kombinasi klasik yang terdiri dari algoritma blocking, permutasi, pemampatan dan vigenere. Ciphertext yang didapatkan disisipkan ke dalam media berupa file gambar berformat bitmap atau jpg 24 bit dengan menggunakan metode LSB. Hasil dari proses penyisipan pesan (embedding) ini adalah file gambar berfornat bmp atau jpg 24 bit, tetapi file gambar tersebut berisi pesan rahasia, sehingga pesan yang dikirim adalah file gambar yang sudah berisi pesan rahasia (stego object).



Gambar. 11. Metode stegano - encode

Pada gambar 12 merupakan proses baca pesan, proses ini dilakukan oleh orang yang menerima pesan rahasia. Pesan yang diterima adalah stego object berupa file gambar berformat bitmap atau jpg 24 bit. Kunci yang digunakan pada proses extracting image adalah kunci yang sama dengan kunci saat enkripsi. Pesan yang masih berupa ciphertext diambil dari file gambar dengan menggunakan metode LSB. Ciphertext harus didekripsi untuk mendapatkan pesan rahasia yang sebenarnya. Ciphertext didekripsi menggunakan algoritma dekripsi kombinasi klasik yang terdiri dari algoritma vigenere, pemampatan, permutasi dan blocking. Dengan demikian, pesan rahasia yang sebenarnya dapat dibaca.



Gambar. 12. Metode stegano - decode

5 IMPLEMENTASI

5.1 Embedding pesan

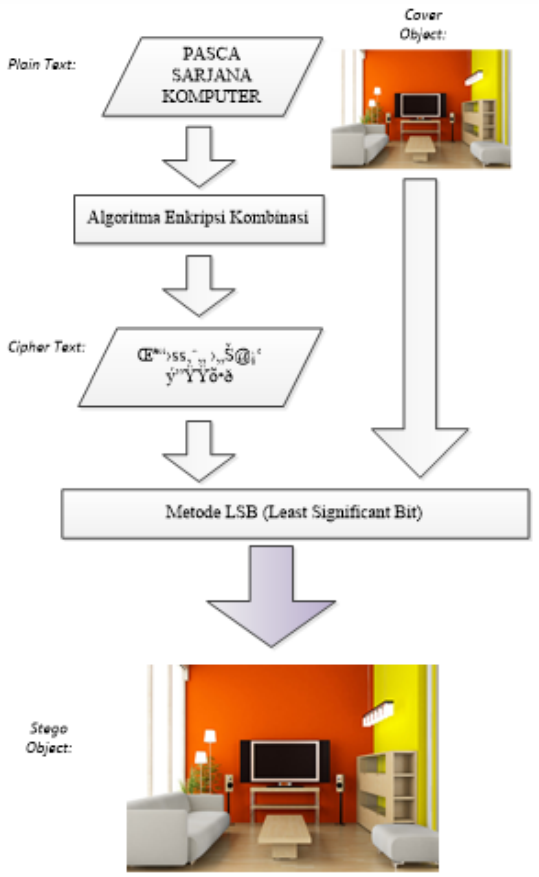
Contoh hasil dari implementasi program untuk penyisipan pesan rahasia adalah sebagai berikut:

Pesan rahasia diubah menjadi karakter yang tidak dapat dipahami maknanya menggunakan algoritma enkripsi kombinasi klasik (terdiri dari blocking, permutasi, pemampatan, dan vigenere) hasilnya disebut dengan ciphertext. Ciphertext disisipkan ke dalam file gambar bitmap atau jpg 24 bit dengan menggunakan metode LSB. Gambar hasil penyisipan pesan rahasia (stego object) dapat disimpan kembali dengan nama yang berbeda. Dari hasil perbandingan antara cover object dan stego object secara fisik tidak tampak adanya perbedaan antara 2 gambar tersebut. Tetapi pesan rahasia tersebut memang telah disisipkan kedalam gambar kedua (stego object) dan hanya dapat dapat ditampilkan kembali dengan metode ekstraksi pesan (extracting).

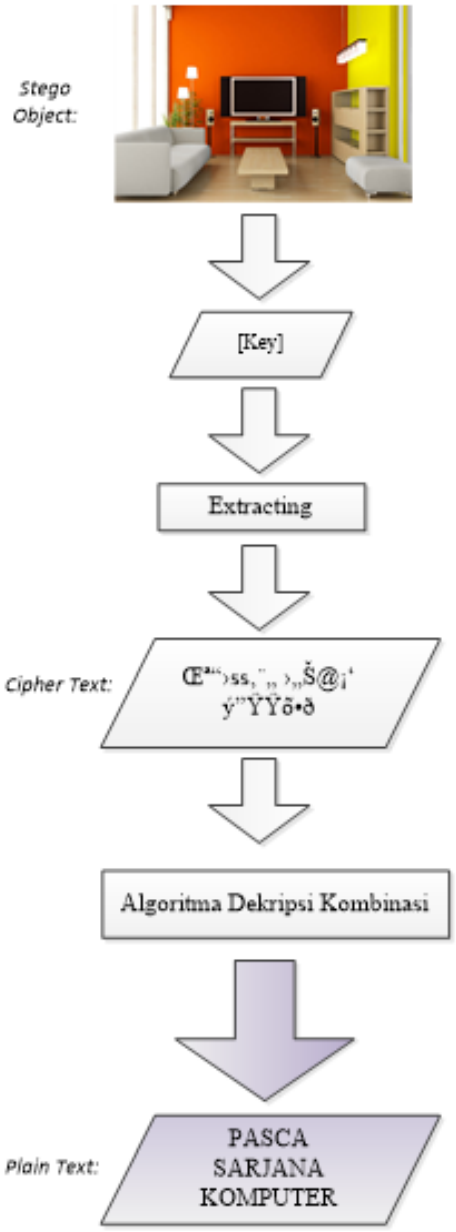
5.2 Ektrasi pesan (extracting)

Contoh hasil dari implementasi program untuk membaca pesan rahasia (extracting) adalah sebagai berikut:

Jika stego object dimodifikasi maka pesan rahasia yang sebenarnya akan hilanag karena nilai RGB pada pixel yang digunakan untuk menyisipkan pesan rahasia berubah. Kelebihan dari teknik steganografi adalah tidak adanya perbedaan yang signifikan antara file gambar sebelum dan sesudah penyisipan. Pesan rahasia tidak dapat dengan mudah didapatkan karena unicode yang digunakan adalah ASCII 256 karakter sehingga pola setiap karakter sulit untuk dilacak.



Gambar. 13. Proses penyisipan pesan rahasia (embedding)



Gambar. 14. Proses ekstrasi pesan rahasia (extracting)

5.3 Hasil citra perbandingan

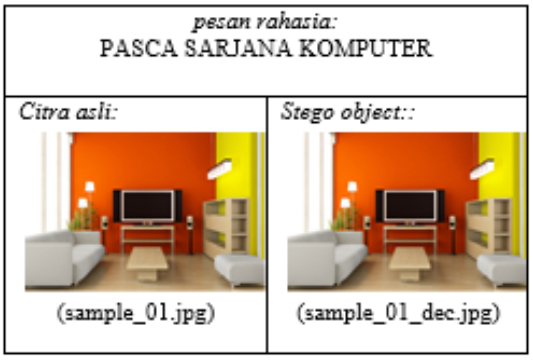
6 KSIMPULAN DAN SARAN

6.1 Kesimpulan

1. Aplikasi ini menggunakan kombinasi algoritma kriptografi klasik blocking, permutasi, pemampatan dan vigenere untuk melakukan enkrip teks sebelum disisipkan kedalam gambar.
2. Aplikasi ini menyembunyikan teks yang telah di enkrip (cipher text) kedalam media citra bmp atau jpg dengan menggunakan metode LSB (Least Significant Bit).
3. Metode Least Significant Bit (LSB) mengubah nilai bit terakhir pada gambar stego cover dengan nilai bit pada pesan teks.
4. Dalam perancangan aplikasi kriptografi klasik kombinasi dan steganografi dengan metode LSB ini menggunakan script makro Excel 2013 dan vba (visual basic application)

6.2 Saran

Sebagai saran yang dapat diberikan dalam perancangan aplikasi ini yaitu:
1. Aplikasi ini dapat digunakan sebagai bahan pembelajaran, terutama hal-hal yang berkaitan dengan kriptografi dan steganografi dengan metode LSB
2. Aplikasi penyembunyian pesan teks tidak hanya diterapkan pada gambar format bmp dan jpg saja, tetapi dapat juga pada gambar format lain, seperti: tif, png, gif dan lain-lain
3. Aplikasi penyembunyian pesan ini dapat diterapkan



Gambar. 15. Perbandingan Citra .JPG

Gambar. 16. Perbandingan Citra .BMP

pada media selain gambar seperti: media audio dan video serta dapat dijalankan pada sistem operasi selain windows 7

4. Dalam merancang sebuah aplikasi penyembunyian pesan teks, penulis mengharapkan metode Least Significant Bit yang diterapkan dengan manggunakan script makro Excel dan vba dapat dikembangkan lebih lanjut dengan bahasa pemrogramman lain seperti: Java, C, visual basic .net dan lain-lain

DAFTAR PUSTAKA

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

[2] David, Murtado A. dan Kasma Utin.Steganografi Gambar Dengan MetodeLeast Significant Bit Untuk Proteksi Komunikasi Pada Media Online. Program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak, 2012.

[3] Maulana, Ahmad Mansur, Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit, PENS-ITS, Surabaya, 2009.

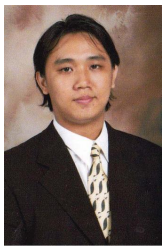
[4] Sasongko, Jati. Pengamanan Data Informasi menggunakan Kriptografi Klasik, Fakultas Teknologi Informasi, Universitas Stikubank Semarang, 2005.

[5] Sutoyo T. Teori Pengolahan Citra Digital, Penerbit: Andi, Yogyakarta, 2009.

[6] Westfeld Andreas. Steganalysis in the Presence of Weak Cryptography and Encoding, Technische Universitat Dresden Institute for System Architecture, Germany, 2006.

Avin Kusuma Putra was born in Nganjuk,east java, Indonesia in 1990. Sekolah Tinggi Teknologi Surabaya college in 2008 and graduated in 2013. Currently working in PT Tempo Inti Media as a programmer. Telp : +62 838 307 31 226.

Suwitno was born in Tangerang, Banten, Indonesia in 1987. Buddhi Dharma University in 2006 and graduated in 2010. Currently working in Buddhi Dharma as a Head of Computer Laboratory.



Yosep Lazuardi was born in Tangerang, Banten, Indonesia in 1987. Dharma Putra STMIK college in 2004 and graduated in 2008. Currently working in PT. Softex Indonesia as a senior programmer.