Implementasi Teknik Steganografi Menggunakan Algoritma Transposisi Columnar

Yeffriansjah Salim
Sistem Informasi, STMIK Indonesia Banjarmasin
Jl. Pangeran Hidayatullah, Banjarmasin, Kalimantan Selatan
yeffri_salim@yahoo,com

INTISARI

Kerahasiaan data sangat diperlukan untuk menjaga dari pihak=pihak yang tidak berwenang agar tidak dapat mengaksesnya, untuk itu diperlukan teknik steganografi dan enkripsi untuk mengaburkan pesan yang dikirimkan ke dalam bentuk gambar / *cover image*. Tujuan utama penelitian ini adalah membuat aplikasi yang berguna memasukan teks / *plain text* yang akan dienkripsi menggunakan kata kunci / *encryption key* menjadi *cypher text* kemudian disisipkan ke dalam *cover image* menjadi *stego object* kemudian hasil dari *stego object* dipisahkan antara *cypher text* dan *cover image*, selanjutnya *cypher text* didekrip menggunakan kata kunci / *encryption key* untuk dapat menghasilkan teks sumber / *plain text*. Metode yang digunakan dalam penelitian ini adalah algoritma transposisi columnar dengan model transposisi 12-21. Hasil yang diperoleh dari penelitian ini membandingkan ukuran file dari gambar yang menjadi *cover image, stego object,* dan gambar hasil dari pemisahan *cypher text* dari *stego object.* Kesimpulan yang diperoleh ukuran file antara *cover image* dan *stego object* tidak mengalami perubahan yang signifikan berapapun jumlah ukuran teks yang disisipkan / *hidden text* ke *cover image* sehingga kriteria Steganografi yakni *Fidelity, Robustness,* dan *Recovery* terpenuhi dengan baik.

Kata kunci *— kriptografi, steganografi, cover image, Stego object, plain text, cypher text, encryption key dan* transposisi columnar.

ABSTRACT

The confidentiality of data is very necessary to protect the party from unauthorized parties so that they cannot access it, for this reason steganography and encryption techniques are needed to obscure the messages sent to them in the form of images. The main purpose of this research is to make an application that is useful to enter text / plain text that will be encrypted using the encryption key to be a cypher text and then inserted into the cover image into a stego object then the results of the stego object are separated between the Cypher text and cover image, then cypher Text is decrypted using an encryption key to produce plain text. The method used in this study is the columnar transposition algorithm with the transposition model 12-21. The results obtained from this study compare the file size of the image that is the cover image, stego object, and the image resulting from the separation of the cypher text from stego object. The conclusions obtained by the file size between the cover image and stego object did not change significantly regardless of the number of sizes of text inserted / hidden text to the cover image so that the Steganography criteria, namely Fidelity, Robustness, and Recovery were fulfilled well.

Keywords *- cryptography, steganography, cover image, Stego object, plain text, cypher text, encryption key and columnar transposition.*

I. PENDAHULUAN

Keamanan data merupakan aspek penting di dalam era teknologi industry 4.0, upaya yang dilakukan dalam melindungi data berupa pesan ataupun isi file dokumen dari orang yang tidak memiliki wewenang atau pembajak data, maka dibutuhkan suatu terobosan teknik kriptografi dan atau steganografi untuk mengatasi gangguan serta meningkatkan keamanan data tersebut, teknik secara umum prinsip nya adalah melindungi keamanan data[1] dengan 5 (lima) kaidah utama adalah faktor *confidentiality, integrity, availability, authenticity,* dan *non-repudiation*. Steganografi sendiri merupakan seni dan ilmu menyembunyikan data menggunakan media lain sebagai *cover* (misalnya gambar / citra) akibatnya data menjadi tidak terlihat / *hidden.* Kriptografi merupakan seni dan ilmu menjaga kerahasiaan data. Pada kriptografi, data / pesan asli diubah menggunakan metode tertentu sehingga sulit dibaca. ilmu steganografi dan kriptografi yang digunakan bersama memperkuat pengamanan data, hal lazim yang dilakukan yaitu melakukan enkripsi pesan (kriptografi), kemudian disisipkan ke dalam media *cover* / gambar (steganografi), pada penelitian ini dilakukan

kriptografi menggunakan algoritma transposisi columnar dalam melakukan implementasi steganografi.

II METODOLOGI PENELITIAN

A Steganografi

Teknik steganografi ini sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan *hieroglyphic* yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia [2]. Steganografi meupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan steganografi adalah rahasia. Istilah Yunani ini berasal dari kata *Steganos*, yang berarti tertutup dan *Graphia*, yang berarti menulis [3].

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Fungsi dari teknik steganografi yaitu sebagai teknik penyamaran *(incognito techniques)* menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas oleh pihak ketiga. Dalam perang Dunia II, teknik steganografi umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman[4]

Kriteria Steganografi

Kriteria steganografi yang harus diperhatikan dalam penyembunyian data, *image*, teks dan suara [5] antara lain :

a) *Fidelity*. Mutu penampung tidak jauh berubah. Setelah penambahan data rahasia, Pengamat tidak mengetahui terdapat data rahasia.
b) *Robustness*. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya).
c) *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*), dimana tujuan steganografi adalah data hiding, data rahasia di dalam penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Ada juga beberapa istilah yang lain yang ada kaitan eratnya dengan steganografi [6], diantaranya:

1. *Hident Text* atau *embedded message* : pesan yang disembunyikan
2. *Covertext* atau *Cover-Object* : pesan yang digunakan untuk menyembunyikan pesan yang sudah tersembunyi (*embedded message*)
3. *Stegotext* atau *stego-object* : pesan yang sudah berisi pesan tersembunyi (*embedded message*).

Steganografi yang menggunakan media gambar *hiddent text* atau *embedded text* yang sudah disisipkan merupakan pesan yang akan disisipkan kedalam *convertext* atau *coverobject*, yaitu berkas dokumen yang digunakan sebagai media penampung berkas kedalam dokumen gambar yang dihasilkan *stegotext* atau *stego-object* yang merupakan sebuah file gambar yang memiliki pesan *embedded*.

B Kriptografi

Menurut kamus bahasa inggris Oxford kriptografi adalah "seni menulis atau pemecahan kode" ini dianggap Sebagai sejarah yang dapat dipertanggungjawabkan sedangkan secara keseluruhan tidak dapat dibatasi pada hal tersebut saja. Selama berabad-abad lamanya definisi kriptografi hanya berfokus pada kode-kode yang memungkinkan untuk digunakan sebagai alat komunikasi rahasia tetapi dewasa ini kriptografi mencangkup lebih dari: hubungan mekanisme untuk kepastian integritas dan teknik untuk bertukar kunci rahasia.

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem Kriptografi (*Cryptosystem*) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi[7]. Menurut Katz, kriptografi adalah studi ilmiah atau teknik untuk mengamankan informasi digital, transaksi dan komputasi yang terdistribusi[8]. Kriptografi bertujuan untuk memberikan layanan keamanan [9] sebagai berikut:

- .
- *Columnar Transposition* merupakan enkripsi yang termasuk mudah untuk terdeteksi oleh kriptanalis dengan melihat jumlah frekuensinya [10]. Kerahasiaan (*Confidentiality*)
- Informasi dirahasiakan dari semua pihak yang tidak berwenang.

- Keutuhan Data (*Integrity*)
- Pesan tidak berubah dalam proses pengiriman hingga pesan diterima oleh si penerima.
- Autentikasi (*Message Autentication*)
- Kepastian terhadap identitas yang terlibat dan keaslian sumber data.
- Nirpenyangkalan (*Nonrepudiation*)

Setiap entitas yang berkomunikasi tidak dapat menolak atau menyangkal atas data yang telah dikirim atau diterima*Columnar Transposition* sendiri merupakan pesan yang ditulis dalam suatu deret yang kemudian dikolomkan. Cara membacanya dari kolom per kolom sesuai kolom yang terpilih. Dalam perang dunia I, Jerman menggunakan *Columnar Transposition* yang disebut ubchi.

Contoh : kata HACKER mempunyai panjang karakter 6 (panjang kolom adalah 6), didefinisikan menurut urutan alphabet dari kata kunci. Dengan menggunakan HACKER menjadi [2 1 4 3 6 5].

Plain Text	A	P	A		K	A	B	A	R		B	A	N	J	A	R	M	A	S	I	N

ENKRIPSI	Keyword	H	A	C	K	E	R

1	2	3	4	5	6
A	P	A		K	A
B	A	R		B	A
N	J	A	R	M	A
S	I	N	#	#	#

Pada *Columnar Transposition* secara umum, semua kolom yang kosong diisi dengan *dummy* seperti pada contoh [###], namun ada juga yang membiarkan kosong. Kelebihan *Columnar Transposition* adalah biasanya algoitma ini digunakan untuk menambah kekuatan dan kerumitan *cipher* lain. Sehingga banyak yang dimodifikasikan dengan *Columnar Transposition.* Kekurangannya algoritma ini paling standar, sangat matematis sehingga proses enkripsi dan dekripsi tidak begitu rumit.

CTC

2	1	4	3	6	5
P	A		A	A	K
A	B		R	A	B
J	N	R	A	A	M
I	S	#	N	#	#
1	2	3	4	5	6

Hasil dari proses enkripsi / *cypher text* ini adalah sebagai berikut :

	1	2	3	4	5	6
Hasil Enkripsi	P A J I A B N S		R # A R A N A A A # K B M #			

Adapun proses dekripsi / *decrypt text* dari enkripsi / *cypher text*

	1	2	3	4	5	6
Hasil Enkripsi	P A J I A B N S		R # A R A N A A A # K B M #			

dengan menggunakan *keyword* / *encryption key* yakni HACKER sebagai berikut :

DEKRIPSI	Keyword	H	A	C	K	E	R

Langkah berikutnya memasukan *cypher text* sesuai dengan jumlah kolom *encryption key* HACKER sebanyak 6 kolom dengan posisi dari atas ke bawah, sehingga tampilannya seperti berikut :

1	2	3	4	5	6
P	A		A	A	K
A	B		R	A	B
J	N	R	A	A	M
I	S	#	N	#	#

Selanjutnya dilakukan *Columnar Transposition* dengan posisi 123456 menjadi 214365 dan proses pembacaan teks dari kiri ke kanan seperti yang terlihat pada gambar berikut ini :

CTC

2	1	4	3	6	5
A	P	A		K	A
B	A	R		B	A
N	J	A	R	M	A
S	I	N	#	#	#

Sampai akhirnya didapatkan hasil dekripsi :

Hasil Dekripsi	A	P	A		K	A	B	A	R		B	A	N	J	A	R	M	A	S	I	N

Proses Enkripsi dan Steganografi :

Proses enkripsi dengan steganografi dilakukan pada penelitian ini :

I. Menentukan gambar yang akan dijadikan *cover image*
II. Menentukan nama file gambar yang akan dijadikan s*tego object*
III. Teks / pesan yang akan disisipkan pada gambar (*cover image*) dilakukan dengan melakukan enkripsi teks / pesan menggunakan kata kunci / *encryption key* dengan algoritma *columnar transposition cipher* sehingga menghasilkan *cipher text* / teks hasil dari proses enkripsi.
IV. *Cipher text* disisipkan ke dalam gambar (*cover image*) sehingga menghasilkan *stego object* disebut dengan proses *encoder*.
V. Proses dekripsi dengan steganografi dimulai dengan menentukan gambar yang merupakan *stego object*,

VI. Menentukan nama file gambar yang akan dijadikan *cover image* hasil pemisahan antara *stego object* dan *cypher text.*

VII. Melakukan proses *decoder* pada *stego object* sehingga memisahkan *cipher text* dari gambar *cover image*

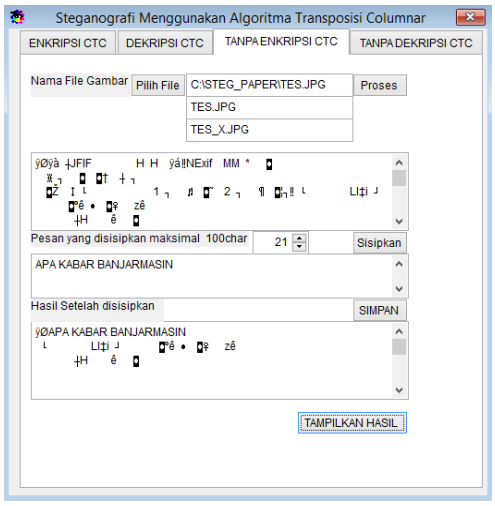
VIII. *Cipher text* dilakukan proses dekripsi menggunakan kata kunci / *encryption key* dengan algoritma *columnar transposition cipher* sehingga menghasilkan *plain text.*

Gambar 1 tahapan proses penelitian

III HASIL DAN PEMBAHASAN

Penelitian dilakukan dengan 2 model :

1. Tidak melakukan enkripsi pesan

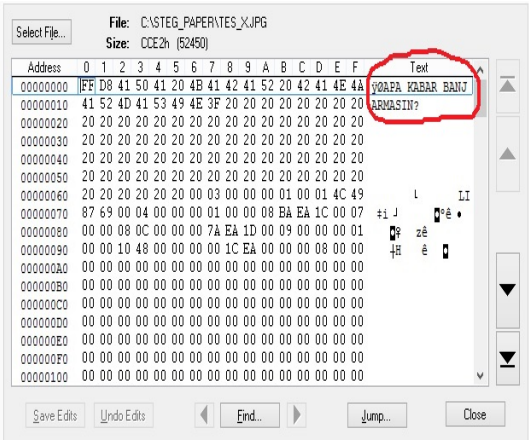


Gambar 2 steganografi tanpa enkripsi

Langkah pertama steganografi tanpa enkripsi menekan tombol **pilihfile** TES.JPG secara otomatis hasil *stego object* TES_X.JPG, tombol **proses** digunakan untuk merubah File menjadi karakter / string, langkah berikutnya mengetikan pesan yang akan disisipkan setelah itu ditekan tombol **sisipkan** akan ditampilkan hasil penyisipan dan tombol **simpan** untuk menyimpan hasil menjadi *stego object.*

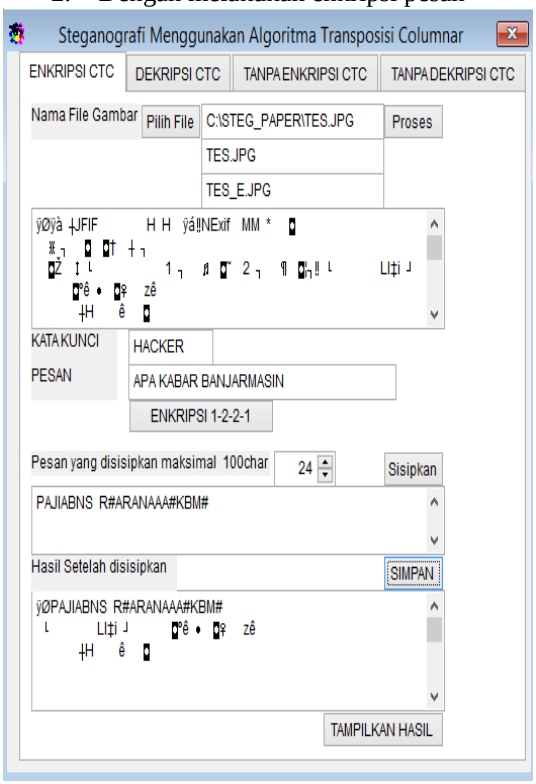
Gambar 3 perbandingan *cover object* dengan *stego object*

Pada gambar 3 di atas tampak perbandingan ukuran *cover object* (TES.JPG) dengan *stego object* (TES_X.JPG) tidak ada perubahan tetap sebesar 52.450 bytes sehingga pengamat tidak curiga adanya pesan rahasia (*Fidelity).* Hasil steganografi pada File TES_X.JPG tanpa proses Enkripsi jika dilihat menggunakan Tools aplikasi bernama HEXEDIT.EXE untuk melihat isi File TES_X.JPG dalam bentuk bilangan Hexadecimal, tampak tulisan dari pesan yang disisipkan yaitu APA KABAR BANJARMASIN, seperti terlihat pada gambar 4 berikut ini :



Gambar 4 isi File TES_X.JPG dilihat dengan Tool HEXEDIT.EXE

2. Dengan melakukan enkripsi pesan

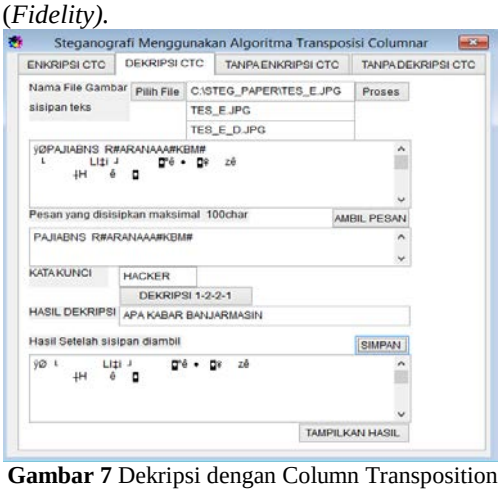


Gambar 5 Enkripsi dengan Column Transposition Cipher

Langkah pertama steganografi dengan Enkripsi Column Transposition Cipher menekan tombol **pilihfile** TES.JPG secara otomatis hasil *stego object* TES_E.JPG, tombol **proses** digunakan untuk merubah File menjadi karakter / string, langkah berikutnya mengetikan kata kunci (*encryption key*) dan pesan yang akan disisipkan, tombol **enkripsi 12-21** ditekan untuk menghasilkan *cypher text*, setelah itu ditekan tombol **sisipkan** akan ditampilkan hasil penyisipan *cypher text* dan tombol **simpan** untuk menyimpan hasil menjadi *stego object.*

Gambar 6 perbandingan *cover image* dengan *stego object*

Pada gambar 6 di atas tampak perbandingan ukuran *cover image* (TES.JPG) dengan *stego object* (TES_E.JPG) tidak ada perubahan tetap sebesar 52.450 bytes sehingga pengamat tidak curiga adanya pesan rahasia (*Fidelity).*



Gambar 7 Dekripsi dengan Column Transposition Cipher

Langkah pertama dekripsi Column Transposition Cipher menekan tombol **pilihfile** TES_E.JPG secara otomatis hasil dekripsi *stego object* TES_E_D.JPG, tombol **proses** digunakan untuk merubah File menjadi karakter / string, langkah berikutnya tombol **ambilpesan** untuk mengambil *cypher text*, Mengetikan kata kunci (*encryption key*), tombol **dekripsi 12-21** ditekan untuk menghasilkan *plain text*, setelah itu ditekan

tombol **simpan** untuk menyimpan hasil dekripsi menjadi *cover image.*

Gambar 8 perbandingan *cover image*, *stego object*, dan *cover image* hasil dekripsi

Hasil perbandingan proses steganografi dengan kombinasi atau tanpa kriptografi columnar transposition cipher dapat dilihat pada gambar 8, sedangkan untuk ukuran, tanggal file hasil ujicoba dapat dilihat pada tabel 1 berikut ini :

TABEL I .
NAMA FILE DAN KETERANGAN

No	Nama File	Keterangan
1	TES.JPG	File Asli
	Ukuran	52450 bytes
	Tanggal dibuat	18-04-2019 03:54:10 PM
	Enkripsi	Column Transposition Cipher
2	TES_E.JPG	Setelah Enkripsi teks disisipkan
	Ukuran	52450 bytes
	Tanggal dibuat	24-04-2019 12:03:22 PM
3	TES_E_D.JPG	Setelah Dekripsi teks pesan
	Ukuran	52350 bytes
	Tanggal dibuat	24-04-2019 12:06:28 PM
	Tanpa Enkripsi	
4	TES_X.JPG	Setelah teks disisipkan
	Ukuran	52450 bytes
	Tanggal dibuat	24-04-2019 12:50:40 PM
5	TES_X_Y.JPG	Setelah teks pesan diambil
	Ukuran	52350 bytes
	Tanggal dibuat	24-04-2019 01:15:02 PM

Kesimpulan

Proses enkripsi *columnar transposition cipher* dikombinasikan steganografi sangat berguna untuk menyamarkan pesan / informasi rahasia, dari beberapa pengujian yang dilakukan besaran kapasitas gambar yang digunakan sebagai *Stego Cover* tidak mengalami penambahan ukuran sebanyak berapapun ukuran teks / pesan yang disisipkan menjadi *Stego Object*, sehingga telah memenuhi kaidah *Fidelity*, *Robustness*, dan *Recovery*.

REFERENSI

[1] R. Popa,.1998.*An Analysis of Steganographic Techniques*, The"Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf

[2] Ariyus, D.2009. *Keamanan Multimedia*. Yogyakarta :Andi Offset

[3] Cox, I., Miller, M., Bloom, J., & Fridrich, J. & .2008. *Digital Watermarking and Steganography 2nd Ed.* Morgan Kauffman., MA.

[4] Munir, Rinaldi. 2006. *Diktat Kuliah IF5054 Kriptografi*. Bandung: Penerbit ITB.

[5] T. Morkel et.all, " *An Overview Of Steganography*", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa

[6] Vembrina, Y. 2006. *Spread Spectrum Steganograpy*. Bandung : Sekolah Teknik Elektro dan Informatika.

[7] Mollin, R. A. 2007. *An Introduction to Cryptography*. 2nd Edition. Chapman & Hall/CRC : Boca Raton, Florida.

[8] Katz, J. & Lindell, Y. 2007. *Introduction to Modern Cryptography*. Chapman & Hall/CRC : United States.

[9] Paar, C. & Pelzl, J. 2010. *Understanding Cryptography*. Springer-Verlag: Berlin.

[10] Kusumaningtyas, Juwita Artanti.2018. *Analisa Algoritma Ciphers Transposition:Study Literature.* Multimatrix Vol I No. 1, Desember 2018. Institut Agama Islam Negeri (IAIN) Salatiga