SIMULASI DAN ANALISIS KEAMANAN TEKS MENGGUNAKAN STEGANOGRAFI LSB DAN CELLULAR AUTOMATA

Jontala Tambunan[1], Ir. Rita Magdalena,M.T.[2], Nur Andini,S.T.,M.T.[3]
[1,2,3]Fakultas Teknik Elektro Telkom University, Bandung
[1]jonthala.tambunan@gmail.com , [2]chaterine.s@gmail.com , [3]andini_dhine@yahoo.com

Abstrak Enkripsi merupakan salah satu metode yang berfungsi untuk mengamankan suatu informasi dengan mengacak informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus mengenai informasi tersebut.

Pada penelitian sebelumnya hanya menyediakan keamanan berupa steganografi atau enkripsi. Dalam tugas akhir ini bertujuan untuk menyediakan dua level tingkat kemanan. Pada level yang pertama menyembunyikan pesan tersebut dengan menggunakan teknik steganografi pada bit terakhir gambar. Pada tingkat kedua mengunakan system 2D *cellular automata*. Dimana hasil dari penyisipan text kedalam gambar tersebut di enkripsi sehingga menghasilkan gambar yang teracak.

Hasil yang diperoleh adalah dengan menggunakan dua level tingkat keamanan terhadap pesan yang dikirim, tingkat keamanan informasi yang dikirimkan lebih tinggi sehingga lebih aman dari penyadapan pesan terhadap pesan yang dikirimkan

.

Kata kunci: Enkripsi, Cellular Automata, Steganografi

Abstract

Encryption is one method that serves to secure any information by making information that cannot read without aid special knowledge.

In the previous research, providing security by aplying steganografy or encryption In this final assignment want to provide two levels of security. . In the first level to hide the message using steganography techniques in the last bit of biner image. In the second level the system using 2D cellular automata. Where the result of the insertion of text into the encrypted image resulting scrambled image.

The result that have been obtain by using 2 level security to the massage to be sent.The level of security of information transmited is higher make the information from eavesdroppers massage. LSB Steganography is resistant to Gaussian noise. Computational time needed to perform image encryption cellular automata method depend on size of the image.

Keywords: Encryption, Cellular Automata, Steganography

1. Pendahuluan

Steganografi merupakan teknik menyembunyikan pesan ke dalam media lain sehingga keberadaan pesan tidak diketahui oleh orang lain[1]. Steganografi berasal dari bahasa Yunani, yaitu *steganos* yang berarti tertutupi atau terlindungi, dan *graphein* yang berarti menulis. Bila disatukan, menjadi "tulisan tersembunyi". Tujuan utama steganografi adalah untuk menjaga kerahasiaan informasi sesungguhnya yang

Pada zaman sekarang ini perkembangan teknologi digital dan multimedia sangat pesat menjadikan pertukaran informasi jarak jauh semakin mudah serta dibutuhkan. Informasi-informasi yang dikirimkan dapat berupa *image,audio,* serta *video*

Suatu informasi sangat penting bagi setiap orang, tetapi disisi lain informasi dapat menjadi ancaman. Ancaman tersebut dapat berupa penyadapan terhadap informasi yang kita kirimkan, sehingga kerahasiaan informasi tersebut menjadi hilang dan dapat membahayakan mereka yang terlibat dalam informasi. Dengan demikian keamanan suatu informasi sangat penting.Untuk mengamankan suatu informasi dibutuhkan suatu sistem keamanan yang dapat melindungi informasi dari pihak-pihak yang ingin menyadap informasi. Sehingga kerahasiaan informasi yang dikirimkan dapat terjaga dan orang yang melakukan pertukaran informasi dapat dengan nyaman menukarkan informasi tersebut. Kemanan sistem dapat dibuat menjadi 1 tingkat kemanan. Akan tetapi dengan memberikan satu tingkat keamanan saja juga masih belum cukup untuk menjaga suatu sistem. Keamanan sistem yang terdiri dari 2 atau lebih sistem keamanan lebih menunjang terjaganya suatu informasi. Steganografi dan Celluar automata merupakan salah satu teknik untuk memberikan keamanan terhadap informasi.

X Steganografi merupakan teknik nenyembunyikan pesan ke dalam media lain sehingga keberadaan pesan tidak diketahui oleh orang lain[1]. Steganografi berasal dari bahasa Yunani, yaitu *steganos* yang berarti tertutupi atau terlindungi, dan *graphein* yang berarti menulis. Bila disatukan, menjadi "tulisan tersembunyi". Tujuan utama steganografi adalah untuk menjaga kerahasiaan informasi sesungguhnya yang.

2. Dasar Teori

2.1 Steganografi

Steganografi merupakan ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh

indera manusia[9]. Media yang umumnya dipakai dalam penyembunyian data dapat berupa teks, citra digital, audio, dan video.

Properti yang digunakan dalam steganografi yaitu[9]:

a. *Embedded message (hidden object)*: pesan yang disembunyikan.
b. *Cover object*: pesan yang digunakan untuk menyembunyikan *embedded message*.
c. *Stego object: cover* yang sudah berisi pesan *embedded message*.
d. *Stego key*: kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari *stego object*.

Gambar 2.1 Proses Steganografi

2.1 Citra dan Citra Digital

Citra merupakan suatu fungsi kontinyu dari intensitas cahaya atau derajat keabuan dalam bidang 2 dimensi yang dapat direpresentasikan dengan f(x,y), dimana x dan y merupakan koordinat spasial dan nilai f(x,y) sebanding dengan skala intensitas cahaya dari citra pada titik tersebut.

2.2 Citra Grayscale

Citra grayscale adalah citra digital yang terbentuk hanya dari warna abu-abu pada tingkatan yang berbeda. Citra ini disebut juga dengan citra 8-bit karena memiliki 2^8 (256) kemungkinan nilai pada masing-masing pixelnya. Nilai tersebut dimulai dari nol untuk warna hitam sampai 255 untuk warna putih.

2.3 Citra Hitam Putih

BW image merupakan pengembangan dari gambar grayscale, dimana gambarnya hanya mengenal dua macam level warna saja, yatu hitam (bit 1) dan putih (bit 0)[2]. Jadi tipe gambar *BW image* tidak mengenal gradasi warna seperti pada tipe gambar *grayscale*.

2.4 Format Citra Bitmap

Di dalam komputer, citra digital disimpan sebagai suatu file dengan format tertentu. Macam-macam format digital, antara lain: Bitmap, JPEG, GIF, PNG, TIFF, PDF, EPS, PCX, dan PSD. Dalam tugas akhir ini, akan digunakan format citra digital Bitmap sebagai citra *cover* dan citra rahasia yang akan disisipkan.

2.2. Cellular Automata

Secara teoritis, cellular automata pertama kali diperkenalkan pada akhir tahun 1940-an oleh John von Neumann dan Stanislaw Ulam sebagai model sederhana untuk mempelajari proses biologi seperti self-reproduction organism. Secara praktis,cellular automata berkembang ketika pada akhir tahun 1960-an John Conway membuat game of life yang mampu memodelkan kehidupan nyata secara sederhana. [2, 1]

3. Perancangan dan Implementasi Sistem

3.1 Identifikasi Kebutuhan Sistem

3.1.1. Spesifikasi Perangkat Keras

Dalam perancangan Sistem steganografi dan kriptografi pada citra digital menggunakan steganografi LSB serta 2D cellular Automata, spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam penelitian tugas akhir ini.

3.1.1 Spesifikasi perangkat keras

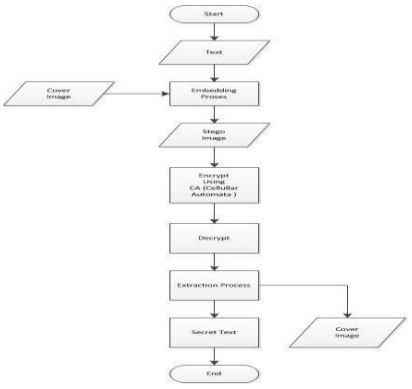
Spesifikasi perangkat keras yang digunakan untuk mengimplementasikan sistem steganografi yang telah dirancang adalah sebagai berikut:

1. Sistem model : HP ProBook 4420s
2. Processor : Intel(R) Core(TM) i3 CPU M 330 @ 2.27 GHz
3. Memory : 2048MB RAM
4. VGA card : Inter(R) HD Graphics (Core i3)

Spesifikasi Perangkat Lunak Spesifikasi perangkat lunak yang digunakan untuk mengimplementasikan tugas akhir ini adalah sebagai berikut:

1. Sistem Operasi Windows 7 32 bit.
2. Programing Tool.
3. Microsoft office excel 2007 untuk mengolah data hasil pengujian system.
4. Mircosoft office visio 2014 untuk membuat diagram blok dan diagram alir..

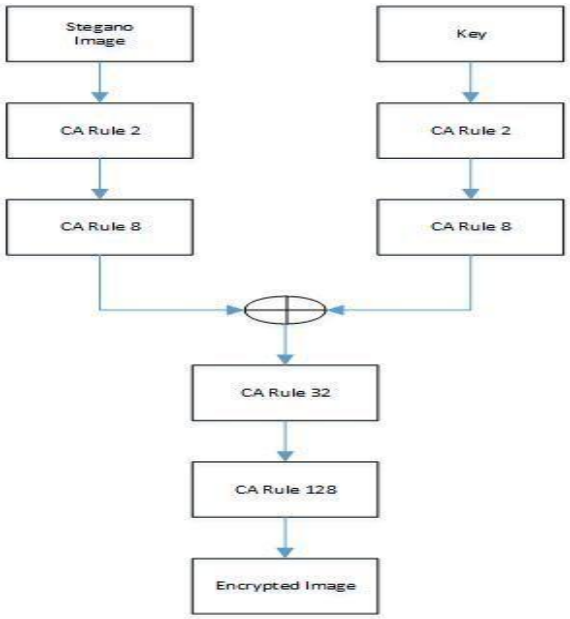
3.2 Perancangan Sistem



Secara umum sistem dapat dijelaskan sebagai berikut. Pada tugas akhir ini, pesan rahasia yang dikirim terlebih dahulu disisipkan ke dalam sebuah cover berupa gambar. Hasil penyisipan tersebut menghasilkan gambar yang berisi pesan rahasia. Kemudian gambar tersebut di enkripsi dan menjadikan gambar tersebut menjadi hancur dan diberikan kata kunci khusus. Hasil enkripsi tersebut dikirim disisi penerima. Kemudian disisi penerima, gambar tersebut diproses untuk mendapatkan pesan rahasia tersebut.

1. Pesan rahasia disisip ke bit terakhir pada gambar yang menjadi cover pesan. Hasil penyisipan tersebut menghasilkan gambar yang telah disisipi pesan rahasia (*stego image*). Dimana orang lain hanya melihat sebuah gambar tanpa mengetahui bahwa di dalam gambar telah disispi sebuah pesan rahasia.
2. Stego image kemudian diuji dengan beberapa serangan.
3. Kemudian stego image kembali diproses untuk melakukan proses enkripsi. Gambar stego image diacak dengan menggunakan *rules* pada 2D Cellular Automata.
4. Kemudian hasil enkripsi kembali diberikan beberapa serangan.
5. Disisi penerima, gambar terenkripsi yang diberi serangan di dekripsi kemudian diekstraksi hasilnya adalah pesan rahasia yang diinginkan serta cover image yang asli. Secret massage hasil ekstraksi inilah yang kemudian dianalisis, apakah sama seperti pesan rahasia yang dikirimkan atau tidak.

3.2.1 Proses Enkripsi



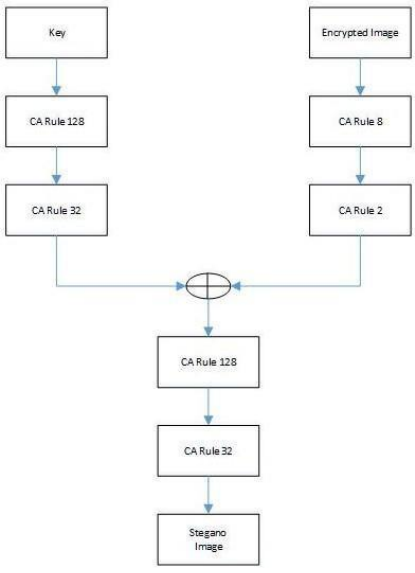
Proses Enkripsi gambar yang terdapat pada gambar diagram blok diatas dapat dijelaskan sebagai berikut:

1. Cover image yang digunakan pada proses penyisipan di sisi penerima adalah citra RGB dengan format bitmap (*.bmp) berukuran 256x256.
2. Pesan rahasia yang dikirim berupa teks.
3. Sebelum dikirim pesan rahasia tersebut terlebih dahulu disisipkan ke dalam cover image. Metode yang digunakan untuk melakukan penyisipan teks pada cover image adalah *Steganography LSB* dimana pesan disisipkan pada bit terakhir cover image.
4. Setelah pesan dikirimkan ke dalam gambar. Gambar tersebut diacak sehingga orang melihat gambar yang teracak dan tidak dapat melihat gambar aslinya.
5. Proses pengacakan dilakukan dengan mengenkripsi cover image dengan metode 2D cellular automata dan untuk melakukan proses enkripsi tersebut dibutuhkan kunci

rahasia yang hanya diketahui oleh pengirim dan penerima pesan.

6. Cover image yang telah disisipi pesan kemudian dienkripsi dengan 2D cellular automata.2D cellular automata yang diterapkaan pertama adalah cellular automata rule 2 begitu juga dengan kunci rahasia untuk melakukan enkripsi diberikan cellular automata rule 2. Setelah itu gambar serta kunci tersebut juga kembali di enkripsi dengan cellular automata rule 8. Kemudian gambar serta key tersebut di xor untuk melakukan pengabungan antara kunci serta cover image. Hasil xor gambar serta key tersebut kembali diberikan cellular automata rule 32 dan cellular automata rule 128.
7. Setelah gambar telah teracak maka gambar siap dikirim ke sisi penerima.

3.2.2 Proses Dekripsi



Proses Enkripsi gambar yang terdapat pada gambar diagram blok diatas dapat dijelaskan sebagai berikut:

1. Penerima menerima CA image dari pengirim dalam bentuk gambar yang telah teracak.
2. Setelah menerima CA image kemudian sisi penerima menentukan CA rule yang digunakan untuk melakukan dekripsi gambar tersebut.
3. Penerima juga harus mengetahui kunci yang digunakan untuk menjalankan proses dekripsi tersebut sehigga proses CA dapat dilakukan
4. Gambar yang telah terekripsi pertama diberikan Cellular automata rule 8 karena proses cellular automata yang terakhir yang digunakan adalah Cellualar automata rule 128 yang merupakan hasil transpose CA rule 8.
5. Setalah itu gambar diberikan lagi Cellular automata rule 2 yang merupakan transpose rule 32
6. Key yang diberikan pada gambar juga diberikan CA rule dimana pertama sekali diberikan CA rule 128 kemudian CA rule 32
7. Setelah gambar dan kunci selesai di CA hasil dari CA kemudian di xor sehigga kunci dan gambar dapat digabung.
8. Setelah itu hasilnya diberikan kembali CA rule 128 dan CA rule 32
9. Kemudian didapatkan stego image yang merupakan sebuah gambar yang berisi pesan.

3. Pengujian dan Analisis Sistem

Pada bab ini membahas tentang pengujian dan analisis dari sistem steganografi citra digital dengan metode *Least Signifikan Bit* serta *Cellular Automata.* Keluaran citra dari sistem ini akan diuji kualitasnya dengan atau tanpa gangguan serta akan dibandingkan hasilnya antara gambar dengan LSB dan CA maupun tidak.

4.1 Lingkup Pengujian

Pengujian pada tugas akhir ini menggunakan 1 buah citra RGB dengan ukuran piksel yang berbeda-beda dengan format Bitmap, yaitu citra yang berukuran 32x32, 64x64, 128x128, 256x256, 512x512 piksel, 9 buah karakter kunci untuk dibentuk menjadi

citra, serta beberapa karakter pesan yang akan menjadi pesan rahasia. Berikut ini merupakan gambar dari citra *cover* yang digunakan dalam pengujian:

4.2 Analisis Data Hasil Pengujian Sistem

Berdasarkan skenario pengujian yang telah ditetapkan sebelumnya maka dilakukan analisis untuk penyisipan mulai dari 32x32 sampai 512x512 citra cover sebagai berikut:

No	Nama	Akurasi Pesan	Jmlh Karakter
1	lena32x32	100	384
		100	192
2	lena64x64	100	1536
		100	728
3	lena128x128	100	6144
		100	3022
4	lena256x256	100	24576
		100	12288
5	lena512x512	100	98304
		100	44152

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari pengujian yang telah dilakukan dalam penelitian kali ini, dapat disimpulkan bahwa:

1. Sistem yang dibangun dapat melakukan proses steganografi dan enkripsi.
2. Steganografi dengan metode LSB mempunyai panjang pesan yang ingin disisipkan bergantung dengan ukuran image yang menjadi cover. Semakin besar ukuran cover image maka semakin banyak pula jumlah karakter yang dapat dikirim menjadi pesan rahasia karena semakin banyak pula bit terakhir yang dapat disisipkan pada pesan.
3. Hasil citra setelah melakukan penyisipan mempunyai tingkat kemiripan yang sama seperti citra awal. Hal tersebut akan mengelabui orang yang dengan kasat mata melihat citra steganografi LSB.
4. Sistem Steganografi LSB tidak tahan terhadap noise Gaussian. Karena hasil ekstraksi pesan setelah diberikan noise berbeda seperti hasil pesan yang rahasia yang dikirimkan.
5. Jumlah karakter mempengaruhi lamanya waktu untuk melakukan proses steganografi LSB.
6. Sistem steganografi LSB mempunyai nilai PSNR <= 52 dB dan akurasi mencapai 100% serta MSE =<0.04 pada karakter maksimum yang dapat disisipkan dalam pesan
7. Sistem steganografi LSB mempunyai nilai PSNR <= 35 dB dan akurasi 0% serta MSE <=21 ketika diberikan noise pada kondisi ketika karakter maksimum yang disisipkan.
8. Berdasarkan hasil subyektif dari para pengamat menggunakan MOS, gambar steganografi sangat mirip dengan citra asli yang menjadi cover pesan rahasia. Sehingga dapat mengelabui orang yang melihat serta gambar stegano yang teracak juga dapat membuat para pengamat tidak mengetahui citra asli dari citra yang telah terenkripsi cellular automata.
9. Waktu komputasi yang dibutuhkan untuk melakukan enkripsi terhadap image. Bergantung pada besarnya gambar yang

akan dienkrip. Semakin besar gambar maka semakin lama pula proses enkripsi begitu juga sebaliknya.

10. Berdasarkan nilai avalanche effect sistem cukup sulit untuk diketahui ketika yang diganti merupakan kata kunci untuk melakukan sistem enkripsi karena terjadi perbedaan yang cukup besar pada bit sebelum dan sesudah pergantian kata kunci. Dimana nilai avalanche yang didapat adalah sebesar 5%.

5.2 Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah:

1. Menggunakan metode steganografi yang berbeda pada system steganografi.
2. Menggunakan enkripsi terhadap pesan rahasia serta gambar.
3. Menggunakan enkripsi terhadap terlebih dahulu baru menyisipkan gambar hasil enkripsi menggunakan metode steganografi.
4. Menggunakan metode enkripsi hybrid cellular automata

DAFTAR PUSTAKA

[1] Kurniawati, Hanna. Cellular Automata: Pemodelan dan Implementasi. Fakultas Ilmu Komputer Universitas Indonesia. 2001.

[2] Schatten, Alexander. Cellular Automata Digital World. http://www.ifs.tuwien.ac.at/~aschatt/info/ca/ca.html. 1999.

[3] Calvianty, Intan Yusantina. 2009. *Multiple Watermarking pada Citra Medis pada Domain Wavelett Menggunakan BCH Encoding.* Bandung: Institut Teknologi Telkom.

[4] Wijaya, Marvin Ch & Agus Prijono. 2007. Pengolahan Citra Digital Menggunakan Matlab *Image Processing Toolbox*. Bandung: Informatika.

[5] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit Informatika.

[6] Green, David G. Cellular Automata. http://life.csu.edu.au/complex/tutorials/tutorial1.html. 1993.

[7] S. Wolfram, "*Cryptography with Cellular Automata in Advances in Cryptology*", Crypto '85Proceedings, Volume 218 of Lecture Notes in Computer Science, Pages 429–432 (SpringerVerlag, Heidelberg, 1986).

[8] Choudhury,Pabitra Pal," *Theory and Applications of Two-dimensional, Null-boundary,Nine-Neighborhood, Cellular Automata Linear rules*", Applied Statistics Unit, Indian Statistical Institute.