ANALISA DAN IMPLEMENTASI TEKNIK KRIPTOGRAFI PADA CITRA DIGITAL MENGGUNAKAN KRIPTOGRAFI VISUAL

ANALYSIS AND IMPLEMENTATION OF CRYPTOGRAPHIC TECHNIQUE IN DIGITAL IMAGE USING VISUAL CRYPTOGRAPHY

Suwitrisna Putra[1], Rita Magdalena[2] , Nur Andini[3].

[1]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik, Universitas Telkom, Bandung

[1]suwitrisnaputra@students.telkomuniversity.ac.id ,[2]ritamagdalena@telkomuniversity.ac.id, [3]nurandini@telkomuniversity.ac.id

Abstrak

Kriptografi Visual merupakan perluasan teknik kriptografi dari secret sharing untuk mengamankan sebuah citra. Secret sharing adalah salah satu metode untuk mengamankan suatu rahasia dengan membagi data tersebut menjadi beberapa bagian yang di sebut share. Tujuan dari pembagian tersebut adalah agar pengguna dapat melindungi kunci tanpa takut terlupa atau hilang. Sebelumnya telah dilakukan penelitian mengenai Kriptografi Visual untuk mengetahui keberhasilan dalam pengimplementasian Kriptografi Visual jika di aplikasikan. Kemudian dilakukan juga penelitian mengenai pengimplementasian Kriptografi Visual pada RGB image . Terdapat juga penelitian bagaimana cara untuk mengembangkan Kriptografi Visual dengan algoritma lainnya dan juga pemanfaatan steganografi pada Kriptografi Visual.

Pada tugas akhir ini akan mencoba mengaplikasikan metoda Kriptografi Visual pada citra digital dan menghitung waktu komputasinya. Enkripsi yang dilakukan adalah pembentukan 2 share dan 4 share. Teknik yang digunakan yaitu eksperimental. Pengimplementasian akan menggunakan software MATLAB R2014a untuk Bahasa pemrogramannya. Pada tugas akhir ini juga akan melihat perbedaan hasil dekripsi pada hasil pembentukan 2 share image dan 4 share image serta dampaknya jika terkena noise.

Pengujian kinerja kriptografi dilakukan dengan membandingkan data dari hasil implementasi 2 share dan 4 share. Data yang dilihat adalah waktu komputasi yang diperlukan untuk keduanya dapat mengenkripsi pesan, kualitas gambar, dan ketahanan noise. Dari hasil pengukuran setelah mencoba pada beberapa citra digital maka diketahui waktu enkripsi berkisar di 2-6 detik untuk 2 share dan 4-10 detik untuk 4 share. Hasil dekripsi pada Kriptografi ini mengalami perbedaan pada saat terkena serangan noise.

Kata kunci : Kriptografi, visual, enkripsi, dekripsi, citra

Abstract

Visual Cryptography is an extension of secret sharing cryptographic techniques to secure an image. Secret sharing is one method for securing a secret by dividing the data into several sections called share. The purpose of the division is so that users can protect the key without fear of forgotten or lost. Previous research has been done on Visual Cryptography to determine the effectiveness and implementation of Visual Cryptography if applicable. Then do also research on the implementation of the RGB image Visual Cryptography. There is also research how to develop Visual Cryptography with other algorithms and also the use of steganography in Visual Cryptography.

In this final task will be to try to apply the method of Visual Cryptography on digital image and calculates computation time. Encryption is done is the establishment of two share and 4 share. The technique used is experimental. The implementation will use MATLAB

R2014a software for programming languages. In this final project will also see the difference on the outcome of the results decryption share the image formation 2 and 4 share the image as well as the impact, if exposed to noise.

Cryptographic performance testing done by comparing data from the implementation of the two share and 4 share. Data that is seen is the computational time required to both be able to encrypt a message, image quality, and noise resistance. From the measurement results after trying on several digital image encryption ranges then known time in 2-6 seconds to 2 seconds for the 4-10 share and 4 share. The result of this cryptography experience the difference at the time of attack from noises.

Keywords : Cryptographic, visual, encryption, decryption, image

1. Pendahuluan

Manusia merupakan makhluk sosial yang saling membutuhkan satu dengan lainnya untuk bertahan hidup, sehingga komunikasi antar manusia tidak akan pernah terputus. Komunikasi yang dilakukan manusia bermacam – macam sesuai dengan kebutuhannya. Seiring berkembangnya jaman, kebutuhan manusia pun meningkat, yang berarti kebutuhan komunikasi pun bertambah. Oleh karena itulah diciptakan berbagai macam peralatan untuk mendukung kebutuhan komunikasi manusia.

Masalah pun muncul dengan adanya teknologi perantara pesan antar manusia tersebut, dibutuhkan keamanan untuk data yang dikirimkan. Nilai penting dari informasi data yang dikirimkan menimbulkan kekhawatiran akan adanya pemalsuan atau peretasan informasi dari pihak ketiga. Teknologi kriptografi mampu menjawab kekhawatiran tersebut karena teknik ini membuat data menjadi sebuah data yang acak, sehingga kecil kemungkinan pihak ketiga bisa meretas atau memalsukan data original yang dikirimkan.

Data yang dikirimkan dewasa ini tidak hanya suara atau tulisan saja, tetapi informasi penting pun bisa berupa gambar. Masalah baru pun muncul dengan jenis data gambar, dimana hasil enkripsi dapat menimbulkan kecurigaan kepada pihak ketiga yang ingin mengambil data tersebut. Untuk menangani hal tersebut, dilakukan berbagai macam penelitian dan pada akhirnya Kriptografi Visual[4] ditemukan. Kriptografi Visual diyakini dapat menangani masalah yang kita hadapi, karena teknik ini merupakan perluasan dari Secret Sharing dan membuat sebuah gambar menjadi beberapa bagian. Bagian bagian tersebut memiliki gambar yang berbeda, tetapi jika disatukan barulah data original tersebut akan muncul. Tidak diperlukan kunci khusus dalam metoda ini, sehingga teknologi ini diyakini mampu menjadi solusi pengamanan data berupa gambar agar tidak mudah di serang oleh pihak ketiga.

Dalam beberapa kasus di dunia Telekomunikasi, keamanan data telah menjadi unsur vital. Oleh karena itulah banyak penelitian terkait Kriptografi Visual dilakukan. Penelitian penelitian sebelumnya mencoba mengembangkan Kriptografi Visual agar dapat digunakan pada citra yang lebih luas maupun metoda mengamankannya. Tetapi pada tugas akhir ini akan dilakukan penelitian terhadap kualitas dan ketahanan Kriptografi Visual 2 share dan 4 share dari kriptografi Visual itu sendiri.

2. Landasan Teori

2.1 Teori Dasar Citra

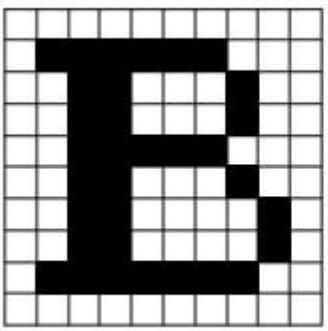
Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek [7]. Ketika sumber cahaya menerangi objek, objek memantulkan cahaya tersebut. Pantulan ini ditangkap oleh alat-alat pengindera optik. Bayangan objek tersebut akan terekam sesuai intensitas pantulan cahaya dan akan menghasilkan citra.

Citra terbagi 2 yaitu bersifat analog dan digital. Citra analog adalah citra yang bersifat kontinu seperti pada televisi. Sedangkan citra digital adalah citra yang dapat diolah oleh komputer. Sebuah citra digital dapat mewakili matriks M kolom dan N baris, dimana ada perpotongan antara kolom dan baris disebut piksel atau *picture element* yaitu elemen terkecil dari sebuah citra.

2.2 Citra Biner

Citra biner (binary image) adalah citra yang hanya memiliki dua buah derajat keabuan : hitam dan putih [6]. Meskipun saat ini citra berwarna lebih disukai karena memberi kesan yang lebih kaya daripada citra biner, namun tidak membuat citra biner mati. Pada beberapa aplikasi citra biner masih tetap dibutuhkan, misalnya logo instansi (yang hanya terdiri atas warna hitam dan putih), citra kode batang (bar code) yang tertera pada label barang, citra hasil pemindaian dokumen teks, dan sebagainya.

Seperti yang sudah disebutkan di atas, citra biner hanya mempunyai dua nilai derajat keabuan : hitam dan putih. Piksel-piksel objek bernilai 1 dan piksel-piksel latar belakang bernilai 0. Pada waktu menampilkan gambar, 0 adalah putih dan 1 adalah hitam. Jadi, pada citra biner, latar belakang berwarna putih sedangkan objek berwarna hitam. Untuk lebih jelasnya dapat dilihat pada Gambar 2.3



0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	1	1	0	0	0
0	0	1	1	0	0	0	1	0	0
0	0	1	1	0	0	0	1	0	0
0	0	1	1	1	1	1	0	0	0
0	0	1	1	0	0	0	1	0	0
0	0	1	1	0	0	0	0	1	0
0	0	1	1	0	0	0	0	1	0
0	1	1	1	1	1	1	1	0	0
0	0	0	0	0	0	0	0	0	0

Gambar 2.3

2.3 Teori Dasar Kriptografi

2.3.1 Pengertian Kriptografi

Kriptografi adalah suatu metode keamanan untuk melindungi suatu informasi dengan menggunakan kata-kata sandi yang hanya bisa dimengerti oleh orang yang berhak mengakses informasi tersebut[1]. Kriptografi merupakan satu-satunya metode yang digunakan untuk melindungi informasi yang melalui jaringan komunikasi yang menggunakan *landline* (kabel di bawah tanah), satelit komunikasi, dan fasilitas *microwave* (gelombang mikro).

Prosedur-prosedur kriptografi juga bisa digunakan untuk authentifikasi pesan, *digital signature*, dan identifikasi pribadi untuk mengotorisasi transfer uang secara digital melalui ATM, kartu kredit, dan melalui suatu jaringan.

Kriptografi sebenarnya adalah suatu metode yang umum digunakan untuk melindungi berbagai macam data yang prosesnya disebut dengan enkripsi, yaitu adalah suatu proses yang mengkonversi sebuah pesan *plaintext* menjadi sebuah *ciphertext* yang bisa dibalik ke bentuk asli seperti semula, yang juga bisa disebut sebagai proses *decoding* atau dekripsi.

2.4 Kriptografi Visual

Kriptografi visual merupakan sebuah skema pembagian yang digunakan dalam distribusi gambar. Kriptografi visual merupakan salah satu perluasan dari secret sharing yang diimplementasikan untuk suatu citra[4]. Seperti halnya teknik kriptografi yang lain, kriptografi visual juga memiliki persyaratan kerahasiaan, integritas data, dan otentikasi. Kriptografi visual yaitu teknik kriptografi data berupa gambar atau citra dengan membagi gambar tersebut menjadi beberapa bagian. Setiap bagian gambar tersebut merupakan subset dari gambar aslinya.

Kriptografi visual pada dasarnya mempresentasikan secret sharing (2,2). Maksudnya skema tersebut menghasilkan 2 (dua) citra pembagi dari gambar aslinya (P) yaitu sebuah gambar hitam putih. Dimana gambar P1 untuk bagian gambar 1 dan P2 untuk bagian gambar 2. P1 dan P2 merupakan distribusi acak dari pixel hitam putih dan tidak menunjukkan informasi apapun. Namun saat P1 dan P2 dilapiskan atau ditumpuk, maka akan didapat informasi seperti gambar aslinya. Apabila hanya ada P1, maka informasi P tidak dapat diketahui tanpa ada P2. Tetapi Kriptografi Visual tidak menutup kemungkinan untuk menciptakan citra pembagi lebih dari 2. Misalkan membuat share sebanyak k dari n, maka konsepnya adalah kita harus bisa membuat share k sebanyak n , sehingga pesan asli baru akan terlihat jika kita menumpuk k sebanyak n, dan tidak akan terlihat jika k ditumpuk kurang dari n.

3. Perancangan

Perancangan sistem dikerjakan dengan beberapa tahap meliputi proses memasukkan citra digital, proses enkripsi citra. Perancangan diawali dengan penggambaran blok diagram kerja system yang menunjukkan cara kerja aplikasi secara umum. Berikut urutan blok diagram sistem :

3.1. Enkripsi

Proses enkripsi pada penelitian ini akan dilakukan sebanyak dua kali percobaan. Percobaan pertama akan mengenkripsi citra digital menjadi 2 buah citra yang tersamarkan.

Citra akan diolah terlebih dahulu agar dapat di enkripsi dengan baik. Yang dimaksud dengan pengolahan adalah perubahan bentuk citra input menjadi sebuah citra biner agar kemudian dapat di proses menggunakan algoritma Kriptografi Visual pada aplikasi MATLAB. Citra tersebut akan di ubah sehingga menghasilkan format .bmp pada saat akan memasuki tahap pengkombinasian piksel.

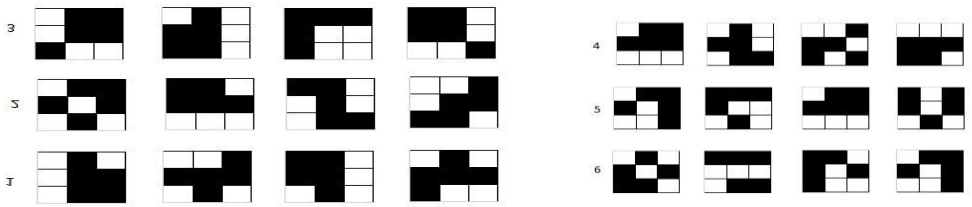
Setelah didapatkan gambar yang di inginkan, gambar tersebut di periksa besar kolom matriksnya untuk kemudian di persiapkan kolom matriks yang sesuai untuk ciphernya, Karena 1 piksel pada plaintext akan menjadi 2x2 piksel pada cipher image. Kolom matriks yang dipersiapkan pun terdapat 2 buah, Karena satu citra asli akan dibagi menjadi 2 buah citra tersamarkan. Setiap matriks 2x2 pada cipher image akan berisikan 2 buah nilai 0 dan 2 buah nilai 1. Adapun kombinasi piksel yang dipersiapkan adalah sebagai berikut :

Kombinasi 1 dan 2 akan digunakan jika piksel yang terdeteksi adalah hitam. Dan kombinasi 3 dan 4 akan digunakan jika piksel yang terdeteksi adalah putih. Hal ini dilakukan dengan tujuan agar memastikan setiap gambar yang tertumpuk akan menghasilkan warna piksel yang di inginkan. Terlihat pada perancangan untuk kombinasi putih meskipun ditumpuk , salah satunya akan tetap menghasilkan warna putih, hal ini dilakukan agar terdapat perbedaan atau tidak semua piksel menjadi gelap pada saat ditumpuk.

Setelah proses tersebut selesai, maka akan di mulai proses pengacakan piksel, setiap piksel pada citra akan di periksa satu persatu, jika piksel tersebut bernilai 1 atau putih, maka akan di ubah menjadi matriks piksel enkripsi untuk blok putih. Jika piksel tersebut bernilai 0 atau hitam, maka akan di ubah menjadi matriks piksel enkripsi untuk blok hitam. Bentuk blok matriks akan berbeda tergantung dengan nilai piksel aslinya. Pengacakan menggunakan random integer dan random permutation pada aplikasi MATLAB. Ini memungkinkan untuk mendapatkan perbedaan penempatan blok cipher yang berbeda pada tiap sharenya sehingga tidak identik atau monoton.

Pada percobaan kedua, citra juga akan diolah terlebih dahulu agar dapat di enkripsi dengan baik. Format citra yang di inginkan tidak jauh berbeda dengan citra 2 share, yaitu .bmp dan setelah citra tersebut siap maka akan memasuki tahap pengkombinasian piksel. Setelah didapatkan gambar yang di inginkan, gambar tersebut di periksa besar kolom matriksnya untuk kemudian di persiapkan

kolom matriks yang sesuai untuk ciphernya. Untuk Kriptografi Visual 4 share, 1 buah piksel pada plaintext akan di ubah menjadi matriks 3x3 piksel pada cipher image. Kolom matriks yang dipersiapkan pun terdapat 4 buah, Karena satu citra asli akan dibagi menjadi 4 buah citra tersamarkan. Setiap matriks 3x3 pada cipher image akan berisikan 5 buah nilai 0 dan 4 buah nilai 1. Hal ini dilakukan agar diperlukan seluruh citra share untuk dapat mengetahui pesan apa yang tersembunyi di dalamnya. Adapun kombinasi piksel yang dipersiapkan adalah sebagai berikut :



Kombinasi 1,2, dan 3 akan digunakan jika piksel yang terdeteksi adalah hitam. Dan kombinasi 4,5,6 akan digunakan jika piksel yang terdeteksi adalah putih. Hal ini dilakukan dengan tujuan agar memastikan setiap gambar yang tertumpuk akan menghasilkan warna piksel yang di inginkan. Setiap 2 tumpuk dari cipher , akan menghasilkan tepat 7 buah piksel hitam. Setiap penumpukan 3 cipher, akan menghasilkan tepat 8 buah piksel hitam, dan penumpukan 4 buah cipher akan tepat menghasilkan 9 buah piksel hitam. Sedangkan terlihat pada perancangan untuk kombinasi putih meskipun ditumpuk , salah satunya akan tetap menghasilkan warna putih, hal ini dilakukan agar terdapat perbedaan atau tidak semua piksel menjadi gelap pada saat ditumpuk.

Setelah proses tersebut selesai, maka akan di mulai proses pengacakan piksel, setiap piksel pada citra akan di periksa satu persatu, jika piksel tersebut bernilai 1 atau putih, maka akan di ubah menjadi matriks piksel enkripsi untuk blok putih. Jika piksel tersebut bernilai 0 atau hitam, maka akan di ubah menjadi matriks piksel enkripsi untuk blok hitam. Bentuk blok matriks akan berbeda tergantung dengan nilai piksel aslinya. Pengacakan menggunakan random integer dan random permutation pada aplikasi MATLAB. Ini memungkinkan untuk mendapatkan perbedaan penempatan blok cipher yang berbeda pada tiap sharenya sehingga tidak identik atau monoton.

3.2 Dekripsi

Setelah proses enkripsi dilakukan, maka selanjutnya akan dilakukan pengujian atau proses dekripsi pada hasil percobaan pertama dan kedua. Proses dekripsi adalah menumpukan citra hasil enkripsi yang terdiri dari beberapa bagian menjadi satu. Proses ini dilakukan untuk melihat apakah proses enkripsi telah sukses dilakukan.

4 Pengukuran dan Analisis

Pada bab ini akan dijelaskan mengenai implementasi masing-masing proses yang telah dijelaskan pada bab sebelumnya.

Untuk menguji teori yang di kemukakan, perlu dilakukan pengujian dengan mengaplikasikan teknik kriptografi visual kepada beberapa gambar dengan menggunakan parameter pengukuran yang berbeda. Hasil dari pengujian ini akan dibandingkan dan kemudian dilakukan analisis terhadap perbedaan yang terjadi.

Pengaplikasian teori akan dilakukan menggunakan program berbasis MATLAB dan dicoba pada 30 gambar berbeda dengan ukuran yang sama agar mengetahui apakah system bekerja dengan baik, maka diperlukan serangkaian pengujian. Hal yang akan dibahas pada bab ini meliputi :

4.1 Lingkungan Implementasi

Percobaan dengan perangkat lunak ini dibangun menggunakan bahasa pemrograman Matlab dan merupakan perangkat lunak berbasis desktop. Spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam proses implementasi perangkat lunak untuk pengelompokkan dokumen ini dijelaskan pada Tabel 4.1.

Tabel 4.1 Spesifikasi Perangkat Keras dan Perangkat Lunak

Perangkat	Spesifikasi
Perangkat Keras	Prosesor : Intel ® Core™ i7-2630QM CPU @ 2.00GHz Memori : 4.00 GB
Perangkat Lunak	Sistem Operasi : Microsoft Windows 10 Perangkat Pengembang : MATLAB R2014a

4.2 Citra Digital

Pengumpulan data citra dilakukan dengan mengumpulkan 30 citra berukuran 300x200, 30 citra berukuran 480x300 dan 30 citra berukuran 600x400, dan setiap citra akan di olah menjadi .bmp pada saat pengimplementasiannya. Setiap citra akan di uji menggunakan Kriptografi Visual 2 share dan 4 share. Setiap percobaan akan menggunakan seluruh citra di atas.

4.3 Implementasi Proses Enkripsi

Pada sub-bab ini akan dijelaskan mengenai proses enkripsi. Terdapat dua buah jenis Enkripsi yang akan dilakukan pada percobaan ini. Aplikasi secret sharing menggunakan algoritma kriptografi visual pada citra biner dengan menggunakan 2 share dan 4 share.

4.4 Implementasi Proses Dekripsi

Proses dekripsi pada kriptografi visual ini adalah dengan cara menumpuk cipher image menjadi satu. Cipher image di pasangkan dengan pasangannya yang tepat dan kemudian akan menunjukan pesan aslinya pada saat gambar telah menjadi satu.

4.5 Pengujian

Dalam sub-bab ini dibahas mengenai pengukuran kinerja algoritma berdasarkan parameter-parameter yang telah ditentukan. Hasil pengukuran setiap algoritma dibandingkan untuk dianalisa perbedaannya. Pengukuran kinerja algoritma yang dilakukan adalah pengukuran waktu komputasi, kualitas hasil dekripsi, dan kualitas hasil dekripsi jika terkena noise. Pengujian dilakukan dengan membandingkan Kriptografi Visual 2 share dan 4 share.

4.5.1 Waktu Komputasi

Pengukuran waktu komputasi dilakukan terhadap seluruh citra digital yang di ujikan. Hal ini dilakukan dengan tujuan mengetahui seberapa baik algoritma Kriptografi Visual jika di implementasikan.Setelah dilakukan percobaan, pengenkripsian citra dengan ukuran 300x200 memakan waktu berkisar di antara 2 detik untuk algoritma Kriptografi Visual 2 Share dan kurang lebih 3 detik untuk mengenkripsi citra dengan ukuran sama menggunakan Kriptografi Visual 4 Share.

Sedangkan untuk ukuran citra 480x300, waktu komputasi yang diperlukan bertambah hingga 2 kali lipatnya, yaitu berkisar pada 4 detik untuk Kriptografi Visual 2 Share dan 6 detik untuk

Kriptografi Visual 4 share. Kemudian setelah dilakukan percobaan ketiga dengan menggunakan citra berukuran 2 kali lipat dari ukuran aslinya, waktu enkripsi bertambah hingga kisaran 6 detik untuk 2 share dan mencapai 10 detik untuk 4 share.

Dapat kita lihat bahwa waktu enkripsi yang diperlukan untuk menciptakan share kriptografi visual tidaklah selalu pasti. Tetapi waktu yang diperlukan berkisar di antara nilai tertentu. Semakin besar gambarnya , maka semakin lama waktu komputasi yang diperlukan, dan begitu juga dengan share yang dibuat. Semakin banyak share yang dibuat, semakin banyak waktu yang diperlukan.

Untuk proses dekripsi, tidaklah jauh berbeda dalam hitungan detik, tetapi tetap saja Kriptografi Visual dengan 2 share memiliki waktu yang relative lebih singkat dibandingkan 4 share. Pada pengenkripsian citra yang lebih besar pun terlihat waktu dekripsi tetap stabil. Tetap berkisar pada 2 detik untuk 2 share dan 3 detik untuk 4 share.

4.5.2 Kualitas Hasil Dekripsi

Pada sub-bab ini akan diperlihatkan perbandingan hasil dekripsi antara Kriptografi visual dengan 2 share dan Kriptografi Visual dengan 4 share. Hal ini bertujuan untuk mengetahui manakah yang lebih baik digunakan jika ingin mendapatkan hasil dekripsi yang lebih baik.

Pada 2 share, gambar terlihat lebih terang dan jelas, sedangkan untuk 4 share, gambar terlihat lebih buram dan bagaikan berada dalam bayangan. Hal ini disebabkan Karena kriptografi visual dengan 4 share menggunakan lebih banyak piksel hitam dalam penyelesaiannya, jika pada 2 share jumlah piksel hitam dan putih memiliki kisaran atau rentang yang sama, pada kriptografi visual 4 share memiliki intensitas warna hitam yang lebih tinggi.

4.5.3 Kualitas Dekripsi Terhadap Noise

Untuk mengetahui kualitas dekripsi , maka dilakukan percobaan ketahanan terhadap noise. Noise yang di berikan ada 3 , yaitu noise Gaussian, Salt & pepper, dan Poisson. Noise diberikan pada Cipher dan kemudian Cipher yang terkena noise akan dicoba untuk di enkripsikan. Dari hasil perhitungan akurasi terhadap noise, pada saat cipher diberikan noise *Gaussian*, gambar hasil dekripsi menjadi sangat buruk

Dari hasil tersebut juga dapat dilihat nilai akurasi akan semakin menurun jika parameter noise yang diberikan semakin besar. Namun nilai akurasi pada cipher yang diberikan noise *Gaussian* Jauh lebih kecil dibandingkan dengan cipher yang diberikan noise *Salt & Pepper*. Hal ini disebabkan sifat dari noise *Gaussian* yang mengubah seluruh nilai pada matriks citra, sedangkan noise *Salt & Pepper* hanya menambahkan nilai di titik atau piksel tertentu saja sehingga nilai yang berubah lebih sedikit. Sedangkan pada saat cipher diberikan noise poisson, hal ini tidak mempengaruhi proses dekripsi atau gambar tidak berubah sama sekali. Hal ini disebabkan oleh karena sifat noise Poisson yang hanya berpengaruh sangat sedikit pada gambar biner.

Maka dapat disimpulkan algoritma Kriptografi Visual tidak dapat bertahan dengan baik jika terserang oleh noise Gaussian maupun Salt n Pepper, tetapi dapat bertahan jika terkena noise Poisson.

5 Kesimpulan dan Saran

5.1 Kesimpulan

Setelah melakukan percobaan terhadap Kriptografi Visual, maka didapatkan kesimpulan berupa :

1. Kriptografi Visual hanya dapat di gunakan terhadap citra digital berbentuk biner saja.
2. Hasil cipher image dari Kriptografi Visual memiliki jumlah piksel yang relative sama, ini mengakibatkan orang awam atau pihak ketiga akan sulit menentukan mana pasangan yang tepat dari cipher tersebut dikarenakan cipher yang terlihat identic satu dengan yang lainnya.
3. Tidak terdapat masalah terhadap besar atau kecil data yang akan di enkripsi oleh Kriptografi Visual, semua dapat terenkripsi dengan baik, hanya saja semakin besar data tersebut maka semakin lama juga waktu komputasi yang diperlukan.

4. Kriptografi Visual memiliki waktu komputasi yang tidak tentu, tetapi memiliki range tertentu tergantung dari ukuran gambar yang akan di enkripsikan. Untuk Kriptografi Visual dengan 2 share memiliki waktu komputasi berkisar 2 detik untuk citra 320x200, 4 detik untuk citra 480x300, dan 6 detik untuk citra 640x400. Sedangkan Kriptografi Visual dengan 4 share memiliki waktu komputasi berkisar antara 4 detik untuk citra 320x200, 6 detik untuk citra 480x300, dan kurang lebih 10 detik untuk citra berukuran 640x400. Dengan demikian kriptografi Visual dengan 2 share memiliki waktu komputasi yang lebih baik daripada Kriptografi Visual dengan 4 share.
5. Tidak terdapat perbedaan yang signifikan pada waktu dekripsi meskipun gambar yang di dekripsikan memiliki ukuran yang berbeda, waktu dekripsi tetap berkisar di antara 2 detik.
6. Kriptografi visual dengan 2 share memiliki kualitas gambar hasil dekripsi yang lebih baik daripada kriptografi visual dengan 4 share, hal ini dikarenakan jumlah perbandingan piksel hitam dan putih pada Kriptografi Visual dengan 2 Share seimbang, dibandingan dengan Kriptografi Visual dengan 4 share yang memiliki rasio jumlah piksel hitam lebih banyak daripada piksel putihnya sehingga membuat gambar dekripsi terlihat lebih buram.
7. Cipher dan hasil dekripsi memiliki ukuran gambar yang lebih besar daripada data aslinya, itu dikarenakan proses Kriptografi Visual membuat piksel gambar asli menjadi beberapa sub-piksel yang berbeda. Ini mengakibatkan terciptanya lebih banyak piksel piksel gambar yang diperlukan.
8. Kriptografi Visual tidak tahan terhadap noise Gaussian dan Salt n Pepper, tetapi memiliki ketahanan tinggi terhadap noise Poisson.

5.2 Saran

Penelitian lebih lanjut diharapkan dapat memperbaiki kekurangan yang ada dan diharapkan dapat mengembangan yang apa yang telah dilakukan pada penelitian ini. Untuk itu disarankan hal-hal berikut.

1. Menggunakan Bahasa pemrograman lainnya seperti java agar mendapatkan perancangan implementasi yang lebih baik lagi.
2. Untuk mendapatkan hasil data yang lebih baik, disarankan untuk lebih teliti lagi dalam memilih citra yang akan digunakan agar mempermudah proses perubahan dan pengenkripsian gambar dan hasil yang terlihat lebih jelas.

DAFTAR REFERENSI

[1] Dony Ariyus, 2008, "Pengantar Ilmu Kriptografi", Penerbit Andi,. Yogyakarta.

[2] Ir.Rinaldi Munir,M.T., 2004, "Pengantar Kriptografi".

[3] L. Hakim, 2014, "Aplikasi Dan Implementasi Secret Sharing Menggunakan Kriptografi Visual Pada Citra Biner".

[4] M. Naor and A. Shamir, 1995, “Visual Cryptography,” *Adv. Cryptogr.*, pp. 1–12.

[5] Putra Darma, 2009, "Pengolahan Citra Digital", Penerbit Andi,. Yogyakarta.

[6] Rinaldi Munir, 2004, "Pengolahan Citra Digital dengan Pendekatan Algoritmik", Bandung : Informatika.

[7] Sutoyo, T, dkk. 2009, "Teori Pengolahan Citra Digital", Penerbit Andi,. Yogyakarta.