IMPLEMENTASI KRIPTOGRAFI DAN STEGANOGRAFI PADA MEDIA GAMBAR MENGGUNAKAN ALGORITMA *BLOWFISH* DAN METODE *LEAST SIGNIFICANT BIT*

CRYPTOGRAPHY AND STEGANOGRAPHY IMPLEMENTATION IN IMAGE USING BLOWFISH ALGORITHM AND LEAST SIGNIFICANT BIT METHOD

Ganesha Dwi A., R. Rumani M., Muhammad Nasrun Prodi S1

Teknik Komputer, Fakultas Teknik, Universitas Telkom Prodi S1

Teknik Komputer, Fakultas Teknik, Universitas Telkom

Prodi S1 Teknik Komputer, Fakultas Teknik, Universitas Telkom

ganesdwiady@gmail.com, rumani@telkomuniversity.ac.id, nasrun@telkomuniversity.ac.id

Abstrak

Di era perkembangan teknologi yang kian pesat saat ini, seluruh aspek kehidupan tidak terlepas dari peran teknologi, khususnya dalam pertukaran informasi. Keamanan dalam pertukaran informasi adalah hal yang patut diperhatikan. Munculnya pihak ketiga, dikhawatirkan melakukan peretasan pada pesan ketika terjadinya pertukaran. Hal ini menjadikan proses enkripsi dan dekripsi data dalam merahasiakan suatu pesan sangatlah penting. Tetapi teknologi kriptografi dirasa masih belum cukup dalam melaksanakan tugas tersebut. Untuk itu diperlukan teknologi steganografi dalam teknik pengamanan pesan. Dalam penelitian ini telah berhasil dibuat suatu implementasi dan kombinasi dari ilmu kriptografi dan steganografi yang optimal dalam pengamanan pesan. Menggunakan algoritma *Blowfish* dalam proses enkripsi, dikombinasikan dengan menyisipkannya melalui media gambar menggunakan metode *Least Significant Bits*. Pemrogramannya diolah dalam bahasa pemrograman *Java* yang cukup populer dan dapat diakses di banyak perangkat teknologi. Hasil Implementasi diuji dengan parameter pengujian PSNR dan pengujian avalanche effect. Dari pengujian didapatkan kesimpulan bahwa implementasi telah berhasil dengan nilai pengujian PSNR berkisar antara 30dB – 40dB dan nilai pengujian avalanche effect berkisar antara 35,94% - 50%.

Kata Kunci : ***Kriptografi, Steganografi, Blowfish, LSB.***

Abstract

In this era, when development of technology increase rapidly, every aspect of our life becomes inseparable from the role of technology, includes the process in exchange of information. The security in the process of exchanging information are things worth to notice . The emergence of a third party is feared for hacking the message when it still in the process of exchanging message. It makes the encryption and decryption process of secret data very essential. But the current cryptographic technology is not enough to carry out the task alone. It requires other technology security techniques such as steganography, in response to these problems. This research has successfully created an implementation and combination of the science of cryptography and steganography. By using the blowfish algorithm for the encryption and decryption process , and combines it with the paste through media images using the least significant bits method. Programming is processed in the Java programming language that is quite popular and can be accessed in many technological devices. The result of implementation is tested with PSNR examination and avalanche effect examination as testing parameters. The conclusion of the test is the implementation has been successful with PSNR examination values ranges between 30dB - 40dB and avalanche effect examination values ranges between 35.94 % - 50 % .

Keyword : ***Cryptography , Steganography , Blowfish , LSB***

1. Pendahuluan

Perkembangan teknologi yang sangat pesat menyokong kebutuhan akses pertukaran data dan informasi dapat dilakukan secara cepat menggunakan teknlogi internet setiap harinya. Nilai penting dari informasi dan data yang terkandung di dalam pesan, menimbulkan kekhawatiran akan terjadinya peretasan ataupun pemalsuan atas pesan tersebut oleh pihak ketiga. Salah satu cara untuk memenuhi kebutuhan proteksi pesan adalah

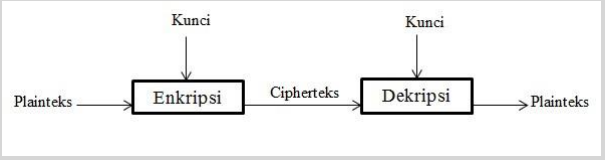
menggunakan teknologi kriptografi.Teknologi kriptografi mampu melakukan enkripsi pesan menjadi data data yang acak. Meskipun sukses dalam memproteksi keamanan data, akan tetapi bentuk enkripsi pesan hasil kriptografi menimbulkan kecurigaan. Hal tersebut membuat peranan teknologi steganografi menjadi esensial. Steganografi adalah suatu teknik penyembunyian pesan pada suatu objek. Pesan hasil enkripsi disisipkan melalui media lain, seperti gambar, lalu ditransmisikan ke tujuannya. Seperti itulah konsep awal dari kombinasi teknologi kriptografi dan steganografi dalam pengiriman dan proteksi pesan.

Blowfish merupakan metoda enkripsi yang mirip dengan DES (DES-like cipher) dan diciptakan oleh Bruce Scheiner[7]. LSB atau *Least Significant Bit* adalah suatu metode steganografi yang memungkinkan penyisipan data pada media gambar. Enkripsi melalui *Blowfish* dan penyisipan menggunakan LSB lalu diimplementasikan menggunakan bahasa pemrograman *Java*. Kombinasi dari ketiga hal tersebut mampu menjadi solusi dalam proteksi dan pengiriman pesan.

2. Dasar Teori

2.1 Kriptografi

Kriptografi (cryptography) secara etimologi berasal dari bahasa Yunani, "cryptos" artinya "secret" (rahasia), sedangkan "graphein" artinya "writing" (tulisan) [4]. Konsep dasarnya adalah memproteksi pesan melalui proses enkripsi, mengubahnya kedalam bentuk tertentu dengan menggunakan kunci pesan yang dirancang secara unik. Tujuannya agar hanya penerima yang memiliki kunci tersebutlah bisa membuka pesan terenkripsi tersebut, proses yang dinamakan dengan dekripsi pesan.



Gambar 2.1 : Skema enkripsi dan dekripsi [4]

Kriptografi juga memiliki beragam aspek dalam tujuannya untuk memberikan layanan keamanan. Aspek aspek yang menunjang hal tersebut adalah sebagai berikut :

1. Kerahasiaan (*confidentiality*), layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak pihak yang tidak berhak [4].
2. Integritas data (*data integrity*), layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman [4].
3. Otentikasi (*authentication*), layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak pihak yang berkomunikasi (*user autenthication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*) [4].
4. Nirpenyangkalan (*non-repudiation*), layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan [4].

2.1.1 Algoritma Kriptografi Modern

Algoritma kriptografi modern beroperasi dalam mode bit, sehingga semua data (baik *key*, *plaintext* maupun *ciphertext*) diproses dalam rangkaian bit biner, 0 dan 1 dengan operasi bit XOR [2]. Algoritma kriptografi modern, berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, dapat dibedakan lagi menjadi tiga jenis [4]. Kriptografi algoritma simetri, kriptografi algoritma asimetri, dan kriptografi algoritma hybrid, termasuk dalam algoritma kriptografi modern.

2.1.1.1 Algoritma Simetri

Kriptografi algoritma simetri memiliki kunci yang sama dalam proses enkripsi dan dekripsi. Sistem kriptografi kunci simetri, mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan [4].Algoritma simetri memiliki kunci yang bersifat rahasia, yang hanya diketahui oleh pihak pihak tertentu (*secret-key cryptography*). Waktu proses enkripsi dan dekripsi algoritma simetri cepat karena efisien dalam pemakaian kunci (hanya terdapat satu kunci dalam prosesnya) [2]. Yang termasuk algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, *Twofish*, *Magenta*, FEAL, SAFER, LOKI, CAST, Rijndael(AES), *Blowfish*, GOST, A5, Kasumi dan lain – lain [7].

2.1.1.2 Algoritma Asimetri

Kriptografi algoritma asimetri adalah algoritma kriptografi yang berbeda kunci untuk enkripsi dan kunci untuk dekripsinya. Hal ini disebabkan kunci untuk enkripsi tidak rahasia, diumumkan ke publik dan dapat diketahui oleh siapa saja (*public-key cryptography*), sementara dalam proses dekripsi, kuncin hanya diketahui oleh penerima pesan (kunci dekripsi bersifat rahasia). Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik [4]. Yang termasuk algoritma asimetri adalah ECC, LUC, RSA, ElGamal dan DH [7].

2.1.1.3 Algoritma Hybrid

Kriptografi algoritma hybrid adalah metode kriptografi yang menggunakan kombinasi antara metode kriptografi algoritma simetri dan kriptografi algoritma asimetri. Proses enkripsi data menggunakan metode simetri karena prosesnya lebih cepat, tetapi kuncinya memakai metode asimetri agar tingkat keamanannya terjamin [2].

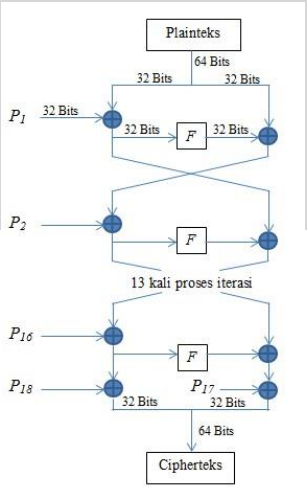
2.1.2 *Blowfish*

Blowfish adalah algoritma kriptografi simetri yang diciptakan oleh Bruce Schneier dengan maksud untuk implementasi pada mikroprosesor skala besar. *Blowfish* memiliki metoda enkripsi yang mirip dengan algoritma kriptografi DES (DES-*like cipher*) [7]. Meski demikian perbandingan hasil evaluasi antara algoritma DES dan algoritma *blowfish*, dengan menganalisa keduanya dari segi keamanan enkripsi, kecepatan proses enkripsi, dan konsumsi daya yang digunakan, didapatkan kesimpulan bahwa algoritma *blowfish* nyatanya lebih cepat dalam melakukan proses enkripsi dibandingkan dengan DES, dengan konsumsi daya yang digunakan juga sama besarnya [6]. Implementasi *blowfish* tidak menggunakan *resource* memori banyak, hal ini menyebabkan algoritma tersebut banyak digunakan pada *embedded system* serta *blowfish* berlisensi bebas paten, sehingga algoritma *blowfish open – source* [2].

2.1.2.1 Algoritma Kriptografi *Blowfish*

Blowfish adalah *cipher* berukuran 64-bit blok dengan kunci yang bervariasi [8]. *Blowfish* memanfaatkan teknik pemanipulasian bit, teknik pemutaran ulang, dan teknik pergiliran kunci yang dilakukan sebanyak 16 kali [2]. Algoritma *Blowfish* terdiri dari dua bagian, yaitu ekspansi kunci dan enkripsi-dekripsi data [8]. Ekspansi kunci mengubah sebuah kunci dengan panjang maksimal 448 bit kepada beberapa *array* sub-kunci dengan ukuran total 4168 *byte* [2].

Enkripsi data terdiri dari fungsi sederhana yang melalui proses iterasi sebanyak 16 kali [8]. Setiap iterasi terdiri dari sebuah permutasi yang bergantung terhadap kunci dan sebuah substitusi yang bergantung pada kunci dan data [8]. Seluruh operasi adalah operasi penambahan dan XOR dalam kata berukuran 32 bit [8]. Satu-satunya operasi tambahan selain itu adalah data *lookup* terhadap *array* dengan empat indeks yang berlaku untuk setiap proses iterasi [8]. *Blowfish* menggunakan sub-kunci dalam jumlah besar, dimana sub-kunci tersebut harus dibangkitkan terlebih dahulu sebelum proses enkripsi dilaksanakan [8].



Gambar 2.2 : Skema enkripsi *blowfish* [8]

2.2 Steganografi

Steganografi (steganography) adalah teknik dalam menyembunyikan pesan dalam pesan, sehingga keberadaannya rahasia dan tidak dapat diketahui, kecuali oleh pengirim dan penerima. Cara kerja pengamanan pesan melalui steganografi menyembunyikan pesan ke suatu media perantara yang aman.

Satu contoh mudah untuk menjelaskan steganografi adalah dengan persoalan tahanan di penjara (*prisoner's problem*) [4]. Misalkan Alice dan Bob ditahan di dalam sel terpisah, dalam sebuah penjara [4]. Satu-satunya cara mereka berkomunikasi hanya melalui surat dengan perantara seorang sipir penjara bernama Fred [4]. Alice menulis surat pada selembar kertas untuk Bob yang tentu saja diserahkan melalui Fred [4]. Fred sudah pasti dapat dan harus memeriksa isi surat tersebut, sebelum disampaikan pada Bob [4]. Hal yang sama juga dilakukan bila Bob akan membalas pesan ke Alice [4]. Misalkan Alice ingin menulis pesan sebagai berikut [4]:

Lari jam satu

Pesan akan langsung dapat terbaca oleh Fred, jika kalimat yang dikirim hanya seperti itu [4]. Misalkan Alice menggunakan kriptografi. Alice melakukan enkripsi pada teks sehingga menjadi cipherteks sebagai berikut [4]:

Xjt#9uvmY!rc$

Fred yang membaca pesan tersebut sudah tentu curiga akan pesan Alice [4]. Solusi terbaik adalah dengan menggunakan steganografi, Alice menyembunyikan pesan rahasia dengan cara menyisipkannya pada setiap huruf pertama di setiap kata dalam sebuah pesan, seperti ilustrasi dibawah ini [4]:

Lupakan **a**sal **r**umor **i**tu, **j**aga **a**gar **m**atamu **s**ehat **a**tau **t**urunkan **u**banmu.

Fred yang menyampaikan pesan mungkin tidak akan curiga dan menganggap pesan ini hanya berupa candaan [4]. Pengamat tidak menyadari bahwa di dalam teks terkandung sebuah pesan rahasia [4].

2.2.1 Konsep dan Terminologi Steganografi

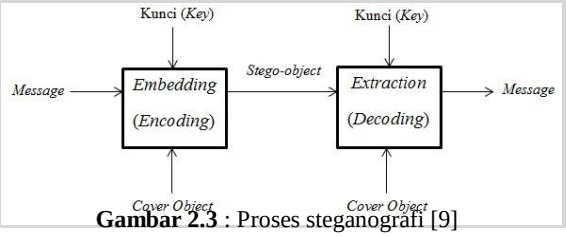
Steganografi umumnya terdiri atas dua buah sistem, yaitu sistem untuk proses penyisipan pesan (*embedding*) dan sistem untuk proses ekstraksi pesan (*extraction*) [9].

Dalam menyembunyikan pesan ada kriteria yang harus dipenuhi, antara lain:

1. *Imperceptbility*, yaitu keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi [4].
2. *Fidelity*, yaitu mutu media penampung tidak berubah banyak akibat penyisipan [4].
3. *Recovery*, yaitu pesan yang disembunyikan harus dapat diungkapkan kembali (*reveal*) [4].

Steganografi memiliki dua macam teknik penyisipan pesan/data ke dalam *cover-object*, yaitu [4]:

1. Ranah spasial/waktu (*spatial/time domain*), teknik ini memodifikasi langsung nilai *byte* dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna *pixel* atau amplitudo) [4]. Contoh metode ini adalah metode *LSB*.
2. Ranah *transform* (*transform domain*), teknik ini memodifikasi langsung hasil transformasi frekuensi sinyal [4]. Contoh dari metode ini adalah metode *spread spectrum*.



Gambar 2.3 : Proses steganografi [9]

2.2.2 *Least Significant Bit*

LSB atau *Least Significant Bit* adalah salah satu teknik penyisipan data dalam steganografi. *LSB* termasuk dalam teknik penyisipan dalam ranah spasial, yang berarti *LSB* memodifikasi langsung nilai *byte* dari *cover-object* [4]. *LSB*, sesuai dengan namanya yaitu *least significant bit*, menggunakan prinsip merubah bit yang paling kurang berarti atau paling terakhir pada susunan bit dalam sebuah *byte* (1 *byte = 8 bit*). Metode Least Significant Bit bahkan mampu digunakan untuk menyembunyikan gambar dalam 24-bit, 8-bit, ataupun yang berformat grayscale [5]. Konsepnya yang sederhana membuat *LSB* menjadi mudah dalam implementasinya untuk digunakan, khususnya untuk kebutuhan dalam dunia steganografi [4].

2.2.2.1. Metode *Least Significant Bit* [4]

Metode *LSB* (*least significant bit*) merupakan metode steganografi yang paling sederhana dan paling mudah diimplementasikan. Untuk menjelaskan metode ini, misalkan *cover-object* yang digunakan berupa citra digital (media gambar). Setiap *pixel* di dalam citra berukuran 1 sampai 3 *byte*. Pada susunan bit di dalam sebuah *byte* (1 *byte = 8 bit*), ada bit yang paling berarti (*most significant bit* atau *MSB*) dan bit paling kurang berarti (*least significant bit* atau *LSB*).

Agar *message* (pesan tersembunyi) tidak dapat dilacak, bit-bit pesan tidak mengganti *byte-byte* yang berurutan, namun dipilih susunan *byte* secara acak. Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan, maka *byte* yang diganti bit *LSB*-nya dipilih secara acak. Pembangkitan bilangan acak seperti *LCG* dapat digunakan sebagai *pseudo-random-number-generator* (*PRNG*). Dalam hal ini, nilai umpan untuk *LCG* berlaku sebagai kunci stegano.

Pesan yang tersembunyi dapat diungkap kembali dengan cara melakukan ekstraksi terhadapnya (*stego-object*). Posisi *byte* yang menyimpan bit pesan dapat diketahui dari bilangan acak yang dibangkitkan oleh *PRNG*. Kunci yang dibangkitkan akan sama, dengan catatan kunci yang digunakan untuk proses ekstraksi sama dengan kunci yang digunakan pada saat waktu penyisipan. Akhirnya bit-bit *message* (pesan rahasia) yang disisipkan secara acak dapat dikumpulkan untuk kemudian diungkap kembali.

2.3 *Peak Signal to Noise Ratio*

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut [3]. PSNR diukur dalam satuan desibel [3]. Standar nilai PSNR untuk citra dengan bit *depth* 8 bit adalah 30dB – 40dB atau lebih [1]. MSE adalah nilai *error* kuadrat rata-rata antara citra *cover* dengan citra tersteganografi [3]. Semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi [3]. Keduanya saling berhubungan dan dapat dijelaskan dengan cara berikut.

$$PSNR = 10.log\left(\frac{MAX^2}{MSE}\right)$$

Gambar 2.4 : Gambar rumus PSNR [3]

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2$$

Gambar 2.5 : Gambar rumus MSE [3]

Dimana [3]:

MSE = Nilai *Mean Square Error* citra steganografi
M = Panjang citra stego (dalam *pixel*)
I(x,y) = nilai piksel dari citra cover
N = Lebar citra stego (dalam *pixel)*
I'(x,y) = nilai piksel pada citra stego

2.4 *Avalanche Effect* [2]

Salah satu karakteristik untuk menentukan baik atau tidaknya suatu algoritma kriptografi adalah dengan melihat *avalanche effect*-nya. *Avalanche effect* merupakan rasio antara jumlah bit-bit *ciphertext* yang berubah akibat perubahan *plaintext* ataupun *key* terhadap jumlah bit total. Perubahan bit-bit *ciphertext* yang kecil pada *plaintext* atau *key* akan menyebabkan perubahan yang signifikan terhadap *ciphertext* yang dihasilkan, dengan kata lain perubahan yang hanya satu bit pada *plaintext* ataupun *key* akan menghasilkan banyak perubahan pada bit *ciphertext*. Jika perubahan bit adalah setengah dari jumlah bit *ciphertext* maka akan sulit bagi *cryptoanalyst* untuk melakukan *cryptanalysis*. Berikut adalah rumus untuk menilai besarnya *avalanche effect*.

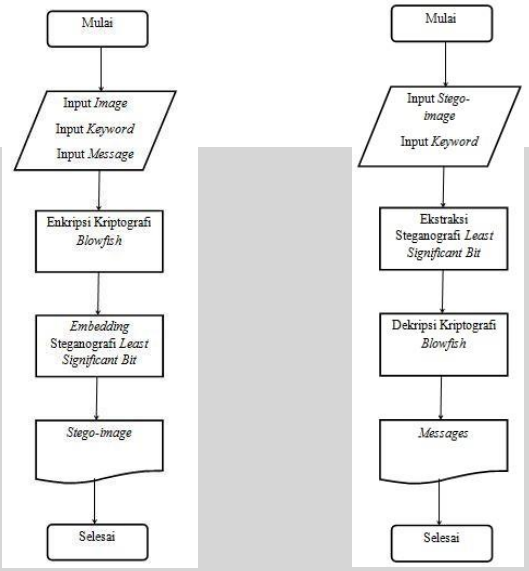
$$avalanche\ Effect = \frac{besar\ perubahan\ bit}{jumlah\ keseluruhan\ bit} \times 100\,\%$$

Gambar 2.6 : Gambar rumus *avalanche effect* [2]

3. Pembahasan

3.1 Diagram Alir Sistem

Berikut adalah gambar yang menjelaskan diagram alir untuk proses enkode (*encode*) dan dekode (*decode*).



Gambar 3.1 : Diagram alir *encode* (kiri) dan diagram alir *decode* (kanan)

3.2 Cara pengujian

Setelah aplikasi selesai dibuat maka dilakukan pengujian - pengujian terhadap aplikasi tersebut. Berikut beberapa parameter uji yang digunakan pada tugas akhir ini.

PSNR

Pengujian PSNR dilakukan untuk menentukan performansi aplikasi dari sisi penyisipan pesan yang dihasilkan oleh *stego-image*.

Ketahanan Citra

Pengujian ketahanan citra. Untuk pengujian ini, dipilih tiga jenis manipulasi pada *stego-image* yang akan diuji, yaitu manipulasi rotasi 180 derajat, manipulasi dengan merubah format *stego-image*, dan manipulasi kompresi dan dekompresi terhadap *stego-image*. Indikator keberhasilan adalah jika *image* hasil steganografi dapat diekstraksi dan pesan yang disisipkan dapat diungkap kembali.

Avalanche Effect

Avalanche effect. Pengujian ini dilakukan untuk menentukan performansi algoritma kriptografi yang digunakan, Pada pengujian ini nilai *avalanche effect* didapat melalui nilai jumlah bit berbeda hasil perbandingan *plaintext* dan *ciphertext*, dibagi dengan total jumlah bit keseluruhan lalu dikonversi dalam bentuk persen.

3.3 Hasil Pengujian

PSNR

Pengujian PSNR dibantu oleh *software PhotoDefiner* PSNR *Calculator*. Pada setiap gambar diberikan *input* berupa pesan sepanjang 128 bit dengan *password* sepanjang 128 bit Berikut adalah tabel lengkap data beserta hasil pengujian PSNR.

Tabel 3. 1 : Pengujian PSNR

No	Nama *File*	Resolusi *File* (*pixels*)		Ukuran *File* (KB)		Perubahan Ukuran *File* (kali ukuran asli)	PSNR (dB)			
		image asli	*stego-image*	*image* asli	*stego-image*		R	G	B	rata rata
1	img1	256 x 192	256 x 192	24	103	4,292	42,466	46,862	41,65	43,659
2	img2	256 x 192	256 x 192	17	77	4,529	48,563	50,498	50,522	49,861
3	img3	256 x 192	256 x 192	37	124	3,351	48,584	49,382	43,309	47,091
4	img4	256 x 192	256 x 192	19	70	3,684	51,724	50,957	48,948	50,543
5	img5	256 x 192	256 x 192	35	105	3	46,43	49,343	43,739	46,504
6	img6	256 x 192	256 x 192	48	113	2,354	40,386	43,21	32,606	38,734
7	img7	256 x 192	256 x 192	47	129	2,745	38,69	44,432	37,926	40,349
8	img8	256 x 192	256 x 192	54	122	2,259	37,464	44,89	35,449	39,267
9	img1	512 x 384	512 x 384	62	374	6,032	46,023	48,648	45,291	46,654
10	img2	512 x 384	512 x 384	44	256	5,818	50,889	51,019	52,833	51,580
11	img3	512 x 384	512 x 384	104	479	4,606	48,78	49,805	45,002	47,862
12	img4	512 x 384	512 x 384	60	268	4,467	52,005	51,017	50,592	51,205
13	img5	512 x 384	512 x 384	100	394	3,94	47,686	49,919	45,97	47,858
14	img6	512 x 384	512 x 384	123	429	3,488	42,004	44,996	35,34	40,78
15	img7	512 x 384	512 x 384	93	481	5,172	42,237	46,994	42,46	43,897
16	img8	512 x 384	512 x 384	119	457	3,840	40,556	46,93	38,35	41,945
17	img1	1024 x 768	1024 x 768	189	1420	7,513	48,955	49,678	48,686	49,106
18	img2	1024 x 768	1024 x 768	150	967	6,447	52,213	51,265	53,975	52,484
19	img3	1024 x 768	1024 x 768	293	1832	6,252	49,508	50,295	47,516	49,106
20	img4	1024 x 768	1024 x 768	210	1101	5,243	52,053	51,034	51,135	51,407
21	img5	1024 x 768	1024 x 768	297	1482	4,990	49,047	50,564	48,166	49,259
22	img6	1024 x 768	1024 x 768	393	1644	4,183	43,92	46,719	39,201	43,28
23	img7	1024 x 768	1024 x 768	230	1679	7,3	46,196	49,106	47,086	47,463
24	img8	1024 x 768	1024 x 768	310	1696	5,471	44,371	48,926	42,026	45,108

Pengujian Ketahanan Citra

Berikut merupakan hasil pengujian ketahanan citra

Tabel 3.2 : Pengujian ketahanan citra

Ukuran Citra *Image*	Ukuran Pesan	Jumlah *Sample*	Rotasi 180 derajat	Format *Image*	Kompresi dan Dekompresi
256x192	32 bit	8	gagal	gagal	berhasil
256x192	128 bit	8	gagal	gagal	berhasil
256x192	512 bit	8	gagal	gagal	berhasil
512x384	32 bit	8	gagal	gagal	berhasil
512x384	128 bit	8	gagal	gagal	berhasil
512x384	512 bit	8	gagal	gagal	berhasil
1024x786	32 bit	8	gagal	gagal	berhasil
1024x786	128 bit	8	gagal	gagal	berhasil
1024x786	512 bit	8	gagal	gagal	berhasil

Avalanche Effect

Berikut adalah hasil dari pengujian *avalanche effect.*

Tabel 3.3 : Pengujian *avalanche effect*

Kasus No	*Plaintext*	*Ciphertext*	*Jumlah bit beda*	*Avalanche effect* (%)
1	sistemkomputer09	suOzs/WCA6b7TOlc	51 bit	39,844%
2	gns123@gmail.com	MA0KJlznbnQameBg	56 bit	43,75%
3	ganesh1104090092	DBAV6h+MmiGA+fEi	60 bit	46,88%
4	ayaOb1ru	Vv45PDBR	32 bit	50%
5	Kupukupu	u621gCg5	23 bit	35,94%
6	bUS8	UxWb	14 bit	43,75%

4. Kesimpulan dan Saran

4.1 Kesimpulan

Beradasar atas hasil proses implementasi, pengujian, dan analisis, didapatkan beberapa poin kesimpulan sebagai berikut.

1. Dari hasil pengujian *black-box* maupun *white-box* dapat disimpulkan bahwa implementasi kriptografi dan steganografi pada media gambar menggunakan algoritma *blowfish* dan metode *least significant bit* telah berhasil dilakukan dengan menggunakan bahasa pemrograman *Java*.
2. Pengujian PSNR pada 24 *sample* menghasilkan nilai PSNR rata rata yang berkisar antara 38 dB hingga 52 dB, sesuai dengan standar nilai PSNR untuk citra dengan bit *depth* 8 bit yang berkisar antara 30dB – 40dB atau lebih. Hal ini membuktikan bahwa algoritma steganografi *least significant bit* memiliki performansi yang cukup baik dan dapat menghasilkan *stego-image* yang berkualitas.
3. Pengujian ketahanan citra juga membuahkan keberhasilan, yaitu pada manipulasi 72 sampel *stego-image* dengan cara kompresi dan dekompresi menggunakan WinRAR. Hal ini menunjukkan bahwa melakukan kompresi dan dekompresi pada *stego-image* dengan menggunakan WinRAR tidak mempengaruhi kemampuan aplikasi untuk mengungkap pesan yang tersisip didalamnya.
4. Pengujian *avalanche effect* pada algoritma kriptografi *blowfish* memberikan hasil yang unik. Dari enam sample pengujian, nilai bit berbeda yang didapatkan berkisar antara 14 bit hingga 60 bit, dengan rentang nilai avalanche effect antara 35,94% - 50%.

4.2 Saran

Saran yang Dalam kontribusi membantu pengembangan perangkat lunak yang memiliki jenis sama, berikut adalah beberapa saran yang dapat diaplikasikan.

1. Pengembangan selanjutnya diharapkan aplikasi ini dapat dikembangkan pada perangkat *mobile*. Aplikasi sejenis ini memiliki potensi untuk menjaga kerahasiaan pertukaran informasi *mobile* seperti pesan sms, *chat*, dan *e-mail*.
2. Untuk segi penggunaan dan pemilihan algoritma diharapkan akan muncul beragam kombinasi berbeda dari kriptografi dan steganografi yang digunakan pada aplikasi serupa dimasa mendatang.
3. Untuk segi penyisipan, diharapkan kedepannya aplikasi ini dikembangkan sehingga mampu menyisipkan data/pesan dalam media *audio* ataupun media *video*.

Daftar Pustaka

[1] Astuti Nugrahaeni, Ratna. 2013. ***Implementasi Kriptografi dan Steganografi untuk Teks pada Media Citra Digital dengan Algoritma AES dan F5***. Bandung : Tugas Akhir Universitas Telkom.

[2] Friska M.P, Martha. 2012. ***Perancangan dan Implementasi Aplikasi Chat Conference pada Komputer Menggunakan Enkripsi Algoritma Blowfish***. Bandung : Tugas Akhir IT Telkom.

[3] Moenandar Male, Ghazali. Wirawan. Setijadi, Eko. 2012. ***Analisa Kualitas Citra pada Steganografi untuk Aplikasi e-Government***. Surabaya : Prosiding Seminar Nasional Manajemen Teknologi XV Program Studi MMT ITS.

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

[5] Neeta, D.. Snehal, K.. Jacobs, D.. 2006. ***Implementation of LSB Steganography and Its Evaluation for Various Bits***. Bangalore : IEEE.

[6] Nie, Tingyuan. Song, Chuanwang. Zhi, Xulong. 2010. ***Performance Evaluation of DES and Blowfish Algorithms***. Wuhan : IEEE.

[7] Rindjani, Rifan. 2006. ***Aplikasi Enkripsi SMS pada Handphone Berbasis Java Menggunakan Algoritma Blowfish***. Bandung : Tugas Akhir STT Telkom.

[8] Scheiner, Bruce. 1996. ***Applied Cryptography***. New York : Wiley.

[9] Tambunan, Jonthala. 2014. ***Simulasi dan Analisis Keamanan Teks Menggunakan Metode Steganografi LSB dan Celular Automata***. Bandung : Tugas Akhir Universitas Telkom.