ISSN : 2407 - 3911

DESAIN OPTIMASI AKURASI ENKRIPSI OBYEK PADA GAMBAR

Muhammad Barja Sanjaya
Program Studi D3 Manajemen Informatika, Fakultas Ilmu Terapan
Telkom University
Jl. Telekomunikasi No.1 - Terusan Buah Batu - Bandung 40257, Jawa Barat, Indonesia
mbarja@tass.telkomuniversity.ac.id

Abstrak

Dewasa ini penerapan teknologi informasi makin maju pesat dalam perkembangannya. Beragam data informasi saling dipertukarkan di internet. Data-data tersebut bisa berupa informasi dalam bentuk format apa saja dan dengan kriteria konfidental yang berbeda. Tingkat kerahasiaan data tersebut bisa didukung dengan adanya implementasi kriptografi yakni enkripsi. Salah satu enkripsi pada data yang sedang ramai dikaji yakni gambar yang memiliki sangat banyak informasi. Proses komputasi kriptografi konvensional pada gambar masih dirasa belum mencapai tingkat performansi yang optimal. Hal ini dikarenakan proses enkripsi yang dilakukan adalah pada keseluruhan gambar sehingga memerlukan biaya komputasi yang mahal. Oleh karena itu pada penelitian ini diusulkan proses inisialisasi sebelum enkripsi dilakukan berupa pemfokusan pada area obyek yang terseleksi saja pada gambar sehingga tidak hanya performansi optimal yang diperoleh namun rasio akurasi juga optimal. Berdasarkan hasil pengujian yang dilakukan, diperoleh adanya rasio akurasi enkripsi pada obyek di gambar sebesar 68,1059% dengan nilai MSE = 0.

Kata kunci: kriptografi, enkripsi, konfidental, inisialisasi, teknologi informasi.

Abstract

The growth of applied information technology nowadays is getting fast. Many information have been exchanged each other in internet. Those data are such as information in any format and different confidentiality criteria. The level of confidentiality can be provided by implementing cryptography process namely encryption. One of encryption process which has been being studied is on image encryption. The process still has high computation costs yet to conduct the encryption due to the process is conducted to the entire of image. Thus in this research, it is proposed an initialization before conducting the encryption such as focusing only on the selected area of object on image. The proposed method is to produce the optimal performance in accuracy ratio. Based on the testing results, it is achieved the percentage of the accuracy of number of selected pixels ratio as big as 68,1059% and the value of MSE = 0.

Keywords: *cryptography, encryption, confidental, initialization, information technology*.

I. PENDAHULUAN

Kriptografi merupakan salah satu teknik untuk mengamankan data sehingga pihak-pihak lain yang tidak berkaitan dan berwenang atau memiliki otoritas tidak dapat mengakses dan membacanya, yakni dengan cara mengacak data (plainteks) tersebut dengan menggunakan persamaan aljabar sehingga keterurutan pada susunan data tersebut berubah dan menghasilkan pesan teracak (cipherteks) (Forouzan, 2008). Penerapan kriptografi jenis apapun juga tidak hanya pada file teks namun juga dapat diimplementasikan pada file gambar yang kaya akan beragam informasi di dalamnya. Suatu gambar memiliki tiga layer yakni merah (R), hijau (G) dan biru (B) (Castelman, 1996). Sehingga proses komputasi pada gambar jelas akan sangat mahal terutama dari sisi waktu pemrosesan dan *memory* yang dibutuhkan untuk memprosesnya (Arya, 2013).

Seiring dengan perkembangan teknologi yang sudah makin maju, beberapa penelitian terkait dengan pemrosesan gambar sudah dipelajari dan dilakukan yakni pada proses pengamanan data dengan cara

mengimplementasikan kriptografi. Beragam jenis kriptografi asimetrik atau pun simetrik sudah diterapkan guna mengacak tiap isi piksel pada gambar. Namun, proses komputasi yang dibutuhkan pada waktu itu tergolong sangattinggi terutama jika diimplementasikan dengan mode *block cipher* yang beroperasi per blok.

Oleh karena itu, untuk pengamanan data pada jenis file berupa gambar perlu dilakukan pemangkasan pada biaya komputasi yang diperlukannya[3]. Biaya pemangkasan tersebut bisa dilakukan dengan cara memfokuskan pada obyek sebenarnya di keseluruhan gambar. Salah satu metode untuk menghasilkan pemilihan atau pemfokusan pada obyek di gambar yakni diperlukannya deteksi tepi pada gambar. Sehingga dengan difokuskannya proses komputasi hanya pada obyek maka waktu proses komputasi dan konsumsi *memory* yang dibutuhkan akan menurun namun tetap dapat menghasilkan *cipher* yang tepat.

Pada penelitian ini diuraikan mengenai suatu desain baru untuk memproses enkripsi pada gambar agar dapat menghasilkan performansi komputasi yang lebih optimal yakni dengan menambahkan proses inisilasisasi berupa deteksi tepi dan proses morphologi pada area obyek di gambar.

II. KAJIAN LITERATUR

Adapun dasar teori dan penelitian sebelumnya terkait yang mendukung penelitian ini sebagai berikut.

II.1 Gambar atau citra

Citra merupakan data dalam bentuk *array* atau tabel atau berupa matriks berukuran dua dimensi (elemen gambar) yang tersusun dalam kolom dan baris. Pada citra *grey-scale* atau dalam format delapan bit, tiap elemen gambar memiliki intensitas nilai yang berkisar dari 0 sampai 255. Pada referensi (Castleman, 1996) dijelaskan bahwa citra yang termasuk ke dalam tipe *grey-scale* adalah citra dengan kriteria warna hitam dan putih.

II.2 *Partially encryption*

Pada penelitian di (Arya, 2013) dilakukan implementasi kriptografi RC4 pada gambar dengan obyek data yang diperoleh dari pemilihan area atau pun keseluruhan pada gambar. Proses kriptografi yang dilakukan digabung dengan *Chaotic Function* untuk menseleksi *bit-bit* yang digunakan untuk menghasilkan kunci key yang diperlukan pada proses enkripsi dan dekripsinya. Dari penelitian, diperoleh hasil bahwa dengan ditambahkannya proses *Chaotic Function* maka proses komputasi lebih cepat dengan kebutuhan *memory* yang masih sama. Serta, dari beberapa hasil uji ditunjukkan bahwa kunci yang dihasilkan dari komputasi *Chaotic Function* lebih aman (*secure*). Adapun hal ini dibuktikannya setelah dilakukan uji pada parameter MSE (*Means Square Error*), PSNR (*Peak Signal to Noise Ratio*), NPCR (*Number of Pixel Change Rate*), dan UACI (*Unified Average Changing Intensity*) (Arya, 2013).

II.3 *Selective bit plane*

Pada penelitian yang dilakukan di (Podesser, et.al, 2002), yakni mengimplementasikan suatu desain untuk memproses kriptografi pada gambar dengan tidak memproses semua *bit* atau *byte* pada piksel yang di gambar, melainkan hanya pada *bit-bit Most Significant Bit* (MSB). Jumlah *bit* MSB yang dipilih tersebut mulai dari satu *bit* pertama, dua *bit* pertama atau 4 *bit* pertama. Hasil dari pengujian dan analisis yang telah dilakukannya ditunjukkan bahwasanya dengan memproses empat *bit* pertama dapat mewakili delapan *bit* atau seluruh *bit* dan menghasilkan cipher yang maksimal (Podesser, et.al, 2002).

II.4 Sobel Operator

Pada penelitian yang dilakukan juga diimplementasikan algoritma deteksi tepi yang bertujuan untuk mendapatkan obyek pada gambar. Salah satu algoritma deteksi tepi yang bisa digunakan yakni operator Sobel. Algoritma ini beroperasi di array dua dimensi sebagai ukuran gradien spasial pada gambar dan menekankan daerah frekuensi spasial tinggi yang sesuai dengan tepi-tepi obyek pada gambar [6]. Adapun konvolusi matriks dari algoritma Sobel sebagai berikut:

1	2	1
0	0	0
-1	-2	-1

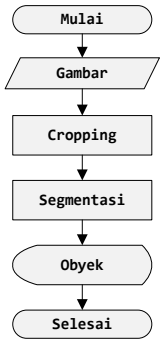
-1	0	1
-2	0	2
-1	0	1

Gambar 1. Sobel Mask [**6**].

III. ANALISIS DAN PERANCANGAN

Adapun desain usulan yang dilakukan pada penelitian ini yakni untuk memangkas biaya komputasi dengan cara tidak memproses area yang

bukan obyek gambar. Proses yang diusulkan adalah dengan memilih area obyek pada gambar yang akan diproses. Berikut adalah gambar *flowchart* yang mendeskripsikan usulan perancangan pada penelitian.



Gambar 2. Usulan perancangan

Penjelasan desain yang dilakukan yakni terdiri dari tahapan diantaranya:

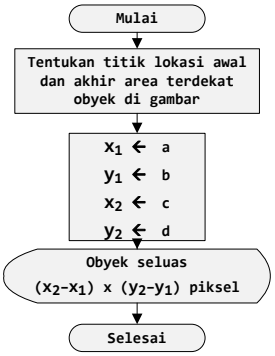
a. ***Load image***

Pada tahapan proses ini dilakukan input data gambar yang akan dilakukan proses berikutnya. Adapun file-file gambar yang akan diproses sebenarnya bisa berupa tipe format file gambar apapun, namun pada penelitian ini ada beberapa kriteria tambahan terkait dengan gambar yang akan diproses, yakni sebagai berikut:

i. Ukuran resolusi gambar yang akan diproses yakni sebesar 400x400 piksel.
ii. Ukuran obyek pada gambar yang dimaksud di poin ke-***i***, yakni sebesar 50x50 piksel.
iii. Warna obyek dan *background* dibedakan dengan warna hitam dan putih.
iv. Pola-pola obyek pada gambar yang dimaksud di poin ke-*i* adalah pola bintang, segitiga, segiempat, trapesium, hati, petir, dan pola di bidang dua dimensi.

b. ***Cropping image***

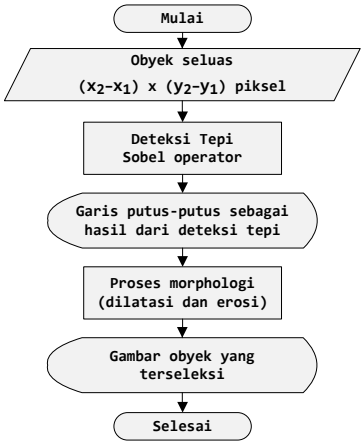
Pada tahapan ini dilakukan pemfokusan area obyek pada gambar yang dimaksud di tahapan ke-***a*** poin ke-***i***. Pemfokusan area dilakukan dengan cara men-*cropping* ke area terdekat dengan obyek dengan bentuk segiempat berukuran seluas ***w***x***h*** piksel. Lebar ***w*** lebih kecil dari lebar gambar utama dan tinggi ***h*** lebih kecil dari tinggi gambar utama. Berikut *flowchart* proses *cropping* image yang dimaksud pada gambar 3 sebagai berikut:



Gambar 3. Proses *cropping* pada gambar

c. ***Edge detection***

Setelah dilakukan *cropping* pada area terdekat dengan obyek, maka dilanjutkan dengan cara melakukan deteksi tepi dengan menggunakan algoritma operator Sobel. Pembanding atau pembeda utama antara gambar obyek yang dimaksud untuk diproses dengan *background* adalah berdasarkan warna. Pada proses ini juga dilakukan operasi morphologi pada garis putus-putus hasil dari deteksi tepi. Operasi morphologi yang dimaksud yakni dilatasi dan erosi yang bertujuan untuk menyatukan kembali garis putus tersebut hasil dari deteksi tepi. Adapun *flowchart* yang menjelaskan proses ini adalah sebagai berikut:



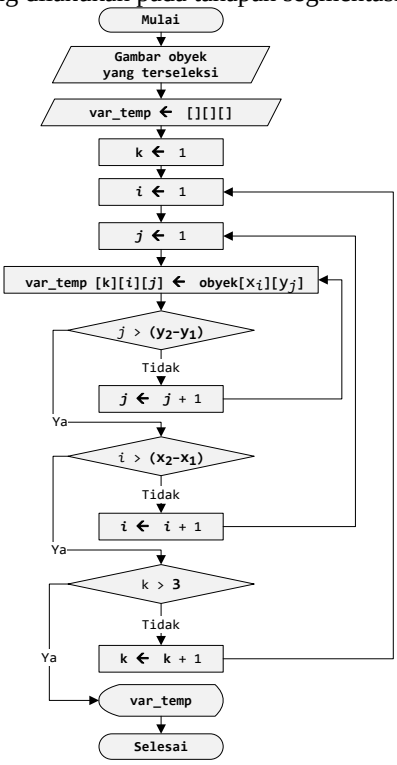
Gambar 4. Proses deteksi tepi

d. ***Segmentation***

Tahapan proses berikutnya yakni dengan menerapkan proses segementasi yang bertujuan untuk memisahkan gambar utama dan area obyek yang telah diseleksi. Hasil proses ini ditampung ke suatu variabel sementara bertipe *array* dimensi dua. Proses ditampungnya area obyek yang sudah diseleksi

sebenarnya merupakan proses penyalinan isi piksel di piksel yang terseleksi.

Berikut gambar *flowchart* yang mendeskripsikan proses yang dilakukan pada tahapan segmentasi



Gambar 5. Proses segmentasi

Adapun pada tahapan ini juga diuraikan mengenai implementasi, hasil dan analisis PEMBAHASANnya terhadap usulan perancangan yang tengah dikaji.

a. **Implementasi**

Pada tahapan implementasi, usulan perancangan diterapkan dan disimulasikan dengan mengaplikasikannya ke dalam aplikasi dengan bahasa pemrograman Matrice for Laboratory (Matlab) versi 2009. Kriteria lengkap lingkungan aplikasi simulasi usulan rancangan sebagai berikut:

i. PC Acer Aspire, E5-474G-53QG
ii. Processor Intel i5-6200U 2.3GHz
iii. Memory DDR3 RAM 4 GB
iv. Memory VGA 2 GB
v. Operating Windows win-10
vi. Matlab r2009a
vii. Microsoft Office Visio 2007

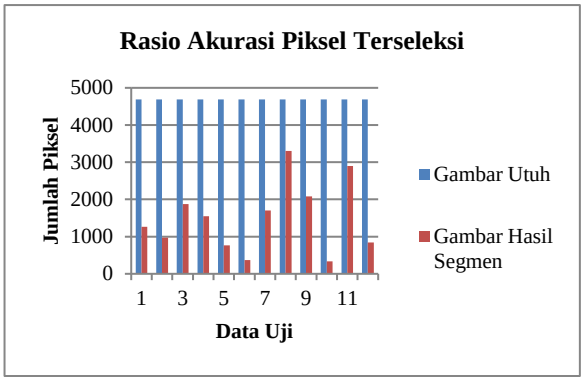
b. **Pembahasan Pengujian**

Berikut ditunjukkan tabel 1 berupa data gambar sebelum dan setelah dilakukan seleksi area terdekat dengan obyek di gambar.

Tabel 1. Daftar hasil uji pada gambar

Gambar pping pada mbar Asli	Gambar Obyek erseleksi	Gambar Hasil egmentasi	Selisih lengan mbar ke-13
		1262	3.428
		974	3.716
		1.871	2.819
		1.548	3.142
		768	3.922
		366	4.324
		1.700	2.990
		3.307	1.383
		2.077	2.613
		334	4.356
		2.902	1.788
		841	3.849
		4.690	0

Adapun selisih jumlah piksel yang terseleksi dari hasil rancangan yang diusulkan dengan metode sebelumnya, disajikan dalam kurva sebagai berikut:



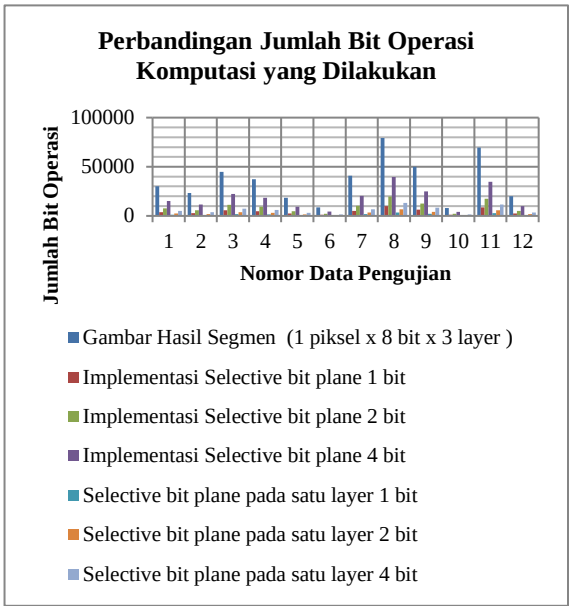
Gambar 5. Rasio akurasi piksel terseleksi

Untuk data lengkap dan rinci mengenai akurasi piksel terseleksi yang dilakukan kombinasi dengan *selective bit plane* biasa dan optimasi disajikan dalam tabel ke-2 berikut:

Tabel 2. Hasil jumlah bit operasi komputasi sebagai plainteks

Nomor Data	Gambar Hasil Segmen (jumlah piksel)	Gambar Hasil Segmen (1 piksel x 8 bit x 3 layer)	Implementasi Selective bit plane			Selective bit plane pada satu layer		
			1 bit	2 bit	4 bit	1 bit	2 bit	4 bit
1	1262	30288	3786	7572	15144	1262	2524	5048
2	974	23376	2922	5844	11688	974	1948	3896
3	1871	44904	5613	11226	22452	1871	3742	7484
4	1548	37152	4644	9288	18576	1548	3096	6192
5	768	18432	2304	4608	9216	768	1536	3072
6	366	8784	1098	2196	4392	366	732	1464
7	1700	40800	5100	10200	20400	1700	3400	6800
8	3307	79368	9921	19842	39684	3307	6614	13228
9	2077	49848	6231	12462	24924	2077	4154	8308
10	334	8016	1002	2004	4008	334	668	1336
11	2902	69648	8706	17412	34824	2902	5804	11608
12	841	20184	2523	5046	10092	841	1682	3364

Juga, bentuk penyajian tabel ke-2 dalam kurva pada gambar ke-6 sebagai berikut



Gambar 6. Perbandingan jumlah bit operasi komputasi sebagai plainteks

c. **Pembahasan**

Berdasarkan tabel dan gambar, diperoleh beberapa analisis yang dijadikan parameter untuk studi penelitian berikutnya, diantaranya:

i. Perbandingan luas area obyek yang akan diproses berikutnya (**rasio**)

Berdasarkan tabel 1 atau gambar 5 ditunjukkan bahwa adanya pengurangan dari isi piksel yang ada pada gambar utama, setelah dilakukan *cropping* dan setelah dilakukan segmentasi. Dari gambar utama dengan ukuran resolusi 400x400 piksel, dilakukan proses *cropping* dengan ukuran 100x100 piksel, dan diperoleh data dengan ukuran lebih kecil yakni 50x50 piksel. Dari data ini juga diperoleh optimasi terhadap data sebenarnya yang akan diproses di berikutnya.

Adapun pengurangan isi piksel tersebut dapat dimodelkan ke dalam suatu model Matematika sederhana. Misalkan luas area gambar utama dinotasikan dengan lambang ***A***, dengan ukuran lebar ***l*** dan tinggi ***t***. Untuk luas area *cropping* dengan lambang ***A***' dan ukuran lebar ***l***' serta tinggi ***t***'. Sedangkan luas area obyek sebenarnya dinotasikan dengan ***A***'' dimana ukuran lebar ***l***'' dan tinggi ***t***''. Semua variabel yang digunakan berada dalam domain bilangan bulat positif dan tak nol. Jika ditinjau dari data yang disajikan pada tabel ke-**1** maka dapat dimodelkan sebagai berikut:

$$l'' < l' < l \text{ dan } t'' < t' < t$$

Sehingga menyebabkan luas daerah yang terseleksi juga makin minimum seperti kriteria sebagai berikut:

$$A'' < A' < A$$

Untuk rataan rasio yang dihasilkan dari pengujian pada semua data gambar diperoleh pengurangan jumlah piksel sebesar 68,1059%. Nilai persentase tersebut diperoleh dari persamaan:

$$\textbf{\textit{rataan}} = \sum_{k=0}^{n} \text{rasio}[k] / \text{n}$$

Dengan *n* = jumlah data, *k* = pencacah tiap data rasio

Sedangkan berdasarkan data pengujian pada implementasi hasil segmentasi obyek pada gambar yang telah dilakukan proses *selective bit plane* biasa diperoleh penghematan biaya komputasi sebesar 50%. Besar penurunan biaya komputasi ini diambil ketika hanya empat *bit* MSB saja yang diproses dan berdasarkan [1] dijelaskan bahwa dengan mengenkripsi empat *bit* MSB sudah dapat mengenkripsi dengan optimal. Selain itu, jika ingin dilakukan optimasi yakni dengan memproses hanya pada salah satu layer, maka diperoleh penghematan lagi sebesar 33.33% namun optimasi yang dilakukan masih memunculkan dugaan data *cipher* yang akan dihasilkan tidak seoptimal yang diproses dengan [1]. Optimasi yang dilakukan pada salah satu layer tersebut bisa menggantikan atau menjadi solusi alternatif jika dibandingkan dengan merusak piksel dengan cara mem-*blurring* sehingga data *cipher* tidak bisa diproses menjadi data plain asli.

ii. Keakuratan pemilihan dan pemilahan area obyek pada gambar (**akurasi**)

Pada parameter keakuratan yang diperoleh berdasarkan hasil yang disajikan di tabel 1 dan tabel 2, terlihat ada beberapa area yang juga masih ikut terseleksi menjadi area obyek. Hal ini terjadi dikarenakan algoritma deteksi tepi yang dipilih juga memiliki ciri khas atau karakteristik tertentu. Serta dari sisi proses morphologi yang dilakukan pada area hasil deteksi tepi juga bisa menjadi faktor berkurangnya performansi dari parameter akurasi. Sehingga dari sisi parameter akurasi obyek yang diperoleh, dapat dikatakan masih belum optimal yang disebabkan adanya area yang bukan obyek juga masih terseleksi. Keoptimalan performansi paling maksimal diperoleh pada hasil pengujian data ke-**6** dan ke-**10**, selain pemilahan dan pemilihan piksel pada area yang tepat juga rasio akurasi yang diperoleh juga tinggi.

iii. Nilai *Mean Square Error* (MSE) pada area obyek hasil segmentasi (*error*).

Untuk nilai MSE yang dihasilkan di gambar segmentasi yakni sebesar 0 (MSE = 0), atau dengan kata lain tidak ada data yang berubah. Hal ini dikarenakan data yang akan diproses sebenarnya adalah pada data variabel hasil salinan dari data di piksel-piksel terpilih bukan proses memanipulasi isi piksel tersebut misal dengan proses steganografi, *watermark*, *blurring* atau komputasi manipulasi lainnya.

Pada tahapan ini hanya sebatas dilakukan penyalinan data piksel dengan koordinat-koordinat piksel yang dilakukan penyalinan ke suatu variabel adalah hasil dari proses *cropping*, deteksi tepi dan morphologi. Nilai MSE ini disertakan juga dengan alasan guna menjamin bahwa tidak ada berubah ketika desain usulan diimplementasikan

IV. KESIMPULAN DAN SARAN

Adapun kesimpulan yang diperoleh setelah melakukan pengujian pada usulan rancangan, sebagai berikut:

1. Adanya penurunan jumlah rasio area yang terseleksi untuk diproses selanjutnya di sisi kriptografi dengan rataan rasio dari keseluruhan data uji sebesar 68,1059%.
2. Tingkat akurasi obyek yang terseleksi dari hasil deteksi tepi dengan operator Sobel beserta proses morphologi yang telah dilakukan masih belum mencapai performansi yang optimal.
3. Tidak ada data yang berubah atau hilang selama dilakukan proses segmentasi dan ditunjukkan bahwa nilai MSE = 0.

Untuk saran penelitian yang memungkikan untuk dilakukan selanjutnya yakni:

1. Merancang modifikasi pada proses *selective bit plane* pada area obyek yang telah diseleksi tersebut.
2. Merancang kriptografi dengan modifikasi pada penjadwalan kunci yang digunakannya.
3. Mengimplementasikan dan mensimulasikan usulan rancangan dengan kriptografi pada

gambar yang dipilih adalah simetrik, yakni *Advanced Encryption Standard* dengan panjang *bit* kunci sebesar 256-*bit*.

4. Memilih, merancang dan mengimplementasikan suatu metode steganografi dengan ditambahkan modifikasi.Referensi ditampilkan sesuai urutan pencantuman pada artikel, bukan berdasarkan alphabet penulis.

REFERENSI

Arya, I Putu Dharmadi. Ari M, Barmawi. Gandeva BS. 2013. "*Enkripsi Gambar Parsial Dengan Kombinasi Metode Stream Cipher RC4 dan Chaotic Function*". Fakultas Informartika, Institut Teknologi Telkom, Bandung.

Castleman, K.R, 1996, Digital Image Processing, Prentice Hall, Englewood Cliffs, New Jersey, 1996

Forouzan, Behrouz. A. 2008. "*Cryptography and Network Security*". International Edition. New York. MacGraw-Hill Companies, Inc.

Podesser, Martina. Schmidt, Hans-Peter, and Andreas Uhl. 2002. "*Selective bit plane Encryption for Secure Transmission of Image Data in Mobile Environments*". School of Telematics & Network Engineering. Carinthia Tech Institute, Klagenfurt, Austria

Ramadevi, Y. Sridevi, T. Poornima, B. Kalyani, B. 2010. "*Segmentation and Object Recognition Using Edge Detection Techniques*". Department of CSE, Chaitanya Bharathi Institute of Technology Gandipet, Hyderabad. International Journal of Computer Science & Information Technology (IJCSIT), Vol 2, No 6, December 2010.

Soleymani, Ali. Md Ali, Zulkarnaen and Nordin, Md Jan. 2012. "*A Survey on Principal Aspect of Secure Image Transmission*". World Academy of Science, Engineering and Technology 66.