



**“PENGEMBANGAN ALGORITMA ENKRIPSI DATA DAN
ANALISIS KEAMANAN MENGGUNAKAN KOMBINASI
DUA CHAOS MAP PADA CITRA WARNA”**

SEMINAR BIDANG KAJIAN

PRIYO SARJONO WIBOWO

99215044

**PROGRAM DOKTOR TEKNOLOGI INFORMASI
UNIVERSITAS GUNADARMA**

2021

DAFTAR ISI

Daftar Isi	i
1. Pendahuluan	1
2. Tinjauan Pustaka	8
3. Metodologi	20
Daftar Pustaka	23

Bab 1

Pendahuluan

1. 1. Latar Belakang

Perkembangan teknologi komputer digital yang semakin cepat melakukan pemrosesan data yang disertai dengan peningkatan kecepatan jaringan internet sebagai penghubung komputer telah memudahkan terjadinya komunikasi berbagai pihak oleh banyak orang di dunia. Hal tersebut memungkinkan terjadinya pertukaran data digital yang dengan mudah dapat dipindahkan, disimpan dan digunakan kembali. Informasi dapat diterima dengan lebih cepat dan dalam berbagai bentuk dengan tujuan penggunaan yang berbeda. Penggunaan kartu kredit, kartu debit, perangkat seluler di dalam kegiatan *e-Commerce*, *e-Government*, *online banking* telah menjadi kebutuhan masyarakat pengguna teknologi digital seiring dengan kemajuan dan perkembangan teknologi komputer digital. Hal ini menimbulkan masalah yang penting, yaitu keamanan data untuk melindungi penyampaian data dari satu tempat ke tempat lain. Bidang ilmu yang mendukung masalah keamanan data adalah kriptografi dan steganografi. Berbagai metode terdapat di dalam kedua ilmu tersebut, bahkan dapat juga menggabungkan kedua metode tersebut untuk mendapatkan solusi terbaik bagi keamanan digital.

Perangkat teknologi digunakan untuk saling bertukar data atau informasi di antara pihak yang terlibat di dalam bentuk pesan digital. Pesan digital dapat berbentuk teks, citra, maupun video yang dikirim dan diterima oleh perangkat digital. Banyak pengguna teknologi ini yang tidak ingin isi pesan digital yang dikirimkan untuk diketahui oleh pihak lain, diantaranya adalah perusahaan, lembaga keuangan, militer, maupun individu yang sangat ingin menjaga kerahasiaan isi pesan digital yang disampaikan agar terhindar dari potensi kerugian karena adanya pencetakan, duplikasi, dan modifikasi isi pesan oleh pihak ketiga, sehingga memerlukan penanganan khusus dalam mengamankan isi pesan digital. Penanganan khusus untuk mengamankan isi pesan digital tersebut guna memastikan terjaganya privasi (privacy), memastikan identitas (authentication), dan ketersediaan (availability) atas isi pesan digital [1]. Oleh karena itu, diperlukan sistem pengamanan data yang mampu menjamin agar isi pesan digital yang dikirimkan melalui jaringan tidak diterima dan diubah oleh pihak yang tidak berhak. Untuk itu telah dikembangkan dalam bidang teknologi informasi cabang ilmu yang mempelajari tentang metode untuk mengamankan isi pesan digital, yaitu kriptografi, steganografi, dan watermarking [3].

1. 2. Batasan dan Tujuan

Kriptografi (cryptography) berasal dari bahasa Yunani yaitu krypto (cryptos) yang berarti menyembunyikan dan graphia (graphein) yang berarti tulisan. Jadi kriptografi berarti tulisan rahasia. Kriptografi [2] adalah ilmu atau seni yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, integritas data, otentikasi data dan otentikasi asal data. Kriptografi dapat diartikan pula sebagai ilmu atau seni untuk menjaga keamanan pesan. Pengembangan dari teknik kriptografi adalah steganografi. Steganografi [1] adalah cabang ilmu yang mempelajari bagaimana menyimpan informasi rahasia di dalam informasi lainnya. Steganografi dapat diartikan sebagai ilmu dan seni yang menyembunyikan keberadaan pesan di dalam pesan lain yang berperan seperti pembungkus, sehingga keberadaan pesan sebenarnya tidak dapat diketahui. Kata steganografi berasal dari bahasa Yunani, yang berarti tulisan tersembunyi. Sedangkan kriptografi berpusat untuk merahasiakan makna pesan. Steganografi dan kriptografi memiliki kesamaan yaitu keduanya digunakan untuk melindungi isi informasi. Kriptografi dan steganografi banyak digunakan bersama dalam mencapai tingkat keamanan tinggi dari suatu data, karena pada perkembangannya, steganografi adalah kelanjutan dari kriptografi.

Metode enkripsi citra telah banyak dikembangkan diantaranya dengan penerapan teori chaos dengan teknik *invisible watermark* terhadap citra [4]. Algoritma yang dihasilkan aman terhadap serangan kriptanalisis, efektif untuk penyandian data citra warna, tetapi untuk citra warna yang berukuran lebih besar, dibutuhkan waktu yang lebih lama untuk melakukan enkripsi dan dekripsi data. Jadi ada peluang untuk menguji kembali untuk citra berukuran yang lebih besar. Penulis yang sama [5], meneliti dengan algoritma Beaufort Cipher, terbukti menghasilkan waktu yang lebih cepat untuk enkripsi dan dekripsi data, efektif dan aman walaupun belum diketahui untuk citra berukuran lebih besar dari 256 x 256 piksel. Algoritma ini cukup menarik untuk diterapkan di dalam alat dengan kemampuan komputasi bergerak seperti *smartphone*. Metode enkripsi chaos Arnold's Cat Map yang diteliti oleh Suryadi MT [8] menghasilkan rata-rata waktu proses enkripsi dan dekripsi berbanding lurus terhadap besarnya piksel citra inputnya. Artinya, semakin besar ukuran piksel maka semakin lama rata-rata waktu untuk melakukan enkripsi dan dekripsi data. Teknik enkripsi citra digital yang menggabungkan Arnold's Cat Map dengan Logistic Map oleh Rinaldi Munir [6], Analisis ruang kunci menunjukkan bahwa jumlah kemungkinan kunci sangat besar sehingga algoritma aman dari serangan *brute-force attack*. Analisis histogram memperlihatkan bahwa histogram dari *cipher-image* berbentuk datar atau terdistribusi *uniform*, sehingga algoritma aman dari

serangan analisis frekuensi. Analisis korelasi memperlihatkan piksel-piksel di dalam *cipher image* tidak berkorelasi satu dengan yang lain (memiliki koefisien korelasi yang mendekati nol), sehingga algoritma aman dari serangan analisis statistik untuk menemukan kunci atau *plain image*. Analisis entropi memperlihatkan algoritma memiliki entropi yang mendekati nilai entropi ideal [7], sehingga algoritma aman dari kebocoran informasi. Analisis sensitivitas menunjukkan bahwa perubahan nilai awal chaos memperlihatkan bahwa algoritma ini aman dari *exhaustive-key search attack*. Penelitian lain [9] oleh Rawat dan Bhandari dengan menggunakan metode steganografi yaitu dengan menyembunyikan citra asli ke dalam citra penyembunyi dengan menyembunyikan bit piksel dari ruang warna RGB ke dalam dua bit signifikan terkecil dari citra pembungkus dan menghasilkan citra stego yang histogramnya secara visual tidak dapat dibedakan dengan histogram dari citra pembungkusnya. Semua penelitian ini terangkum dalam tabel 1 di bawah ini.

Tabel 1. Tinjauan Penelitian Sebelumnya

Penulis / Tahun	Topik	Hasil	Keterbatasan	Prospek
Naniek Widyastuti/2014	Penerapan teori chaos dengan algoritma Beaufort Cipher terhadap citra	Algoritma ini efektif, aman, proses cepat untuk enkripsi dan dekripsi data (0.7 detik), namun hasil visual pada histogram masih terlihat adanya intensitas warna pixel yang kurang merata, sehingga masih dimungkinkan terjadinya serangan menggunakan statistical attack	Belum diketahui penerapan untuk citra berukuran lebih dari 256 x 256 piksel	Pengembangan teknik untuk perangkat lebih kecil, seperti smartphone.
Naniek Widyastuti, Emy Setyaningsih/2014	Penerapan teori chaos dengan teknik <i>invisible watermark</i> terhadap citra	Algoritma enkripsi yang dirancang aman terhadap serangan kriptanalisis dengan rata-rata	Memerlukan waktu yang lama utk citra berukuran besar	Pengujian kembali untuk citra berukuran besar.

		<p>nilai entropi mendekati 8. Algoritma ini cukup efektif untuk penyandian data citra warna. Terlihat hasil visual pada histogram intensitas warna pixel yang lebih merata. Untuk citra dengan ukuran sebesar dua kali ukuran membutuhkan waktu proses tiga kali lipat untuk enkripsi maupun dekripsi data.</p>		
<p>Suryadi MT, Zuherman Rustam, Wiwit Widhianto/ 2014</p>	<p>Enkripsi citra digital skema transposisi berbasis fungsi chaos yaitu Arnold's Cat Map.</p>	<p>Rerata waktu proses enkripsi dan dekripsi relatif sama, berbanding lurus terhadap ukuran piksel citra inputnya. Jika ukuran piksel suatu citra maka semakin besar, maka akan semakin lama rata-rata waktu yang akan dibutuhkan untuk proses enkripsi dan dekripsi data.</p>	<p>Waktu yang lama untuk citra yang berukuran besar</p>	<p>Pengujian dengan metode chaos map yang lain dan membandingkannya dengan hasil penelitian ini.</p>
<p>Rinaldi Munir / Juli 2012</p>	<p>Teknik enkripsi citra digital yang menggabungkan Arnold's Cat Map sebagai teknik permutasi untuk</p>	<p>Analisis ruang kunci menunjukkan bahwa jumlah kemungkinan kunci sangat besar sehingga algoritma aman</p>	<p>Belum diketahui penerapan untuk citra dengan ukuran lebih dari 512 x 512 piksel</p>	<ul style="list-style-type: none"> ▪ Menguji kembali untuk citra yang lebih besar, ▪ Penggunaan nilai parameter yang berbeda pada teknik Logistic map

	<p>mengacak piksel-piksel dalam citra dan teknik Logistic Map sebagai teknik substitusi untuk membangkitkan keystream dan penerapan teknik selektif</p>	<p>dari serangan brute-force attack. Analisis histogram memperlihatkan bahwa histogram cipher-image berbentuk datar atau terdistribusi uniform, sehingga algoritma aman dari serangan analisis frekuensi. Analisis korelasi memperlihatkan piksel- piksel di dalam cipher-image tidak berkorelasi satu dengan yang lain (koefisien korelasinya mendekati nol), sehingga algoritma aman dari serangan analisis statistik untuk menemukan kunci atau plain-image. Analisis entropi memperlihatkan algoritma memiliki entropi yang mendekati nilai entropi ideal (8), sehingga algoritma aman dari kebocoran informasi, Analisis sensitivitas menunjukkan</p>		
--	---	--	--	--

		bahwa perubahan nilai awal chaos memperlihatkan bahwa algoritma ini aman dari exhaustive-key search attack.		
Deepesh Rawat, Vijaya Bhandari/Februari 2013	Teknik steganografi dengan menyisipkan piksel dari citra warna asli ke dalam piksel citra warna pembungkus pada posisi dua bit signifikan terkecil (least significant bits) dengan tujuan agar citra asli tidak terdeteksi keberadaannya.	Analisis histogram memperlihatkan bahwa histogram citra pembungkus secara visual tidak terlihat adanya perubahan karena adanya penyisipan citra warna asli.	Belum diketahui ukuran citra yang digunakan pada penelitian.	<ul style="list-style-type: none"> ▪ Pengukuran kinerja untuk berbagai ukuran citra ▪ Pengkombinasian dengan teknik kriptografi untuk menghindari pendeteksian penyandian pesan yang terenkripsi

Beberapa hal masalah yang dapat dirumuskan, yaitu:

1. Usulan algoritma chaos map yang sesuai untuk mempercepat waktu enkripsi dan dekripsi pada citra warna yang berukuran besar.
2. Metode chaos map apakah yang dapat melakukan perbandingan teknik enkripsi pada citra warna.
3. Metode apakah yang paling baik sehingga dapat memberikan tingkat akurasi yang tinggi dalam analisis teknik chaos pada citra warna.
4. Sejauh mana kemungkinan pengkombinasian salah satu teknik kriptografi di atas dan steganografi yang lebih sesuai diimplementasikan pada gawai dengan spesifikasi perangkat keras lebih rendah dari PC, misalnya pada smartphone.

Berdasarkan hasil penelitian yang telah dilakukan oleh para peneliti seperti yang telah diuraikan di atas, terlihat masih adanya peluang untuk melakukan pengembangan algoritma yang lebih baik untuk melakukan enkripsi dan dekripsi berdasarkan fungsi chaos, sehingga

diharapkan akan mendapatkan algoritma terbaik dengan melakukan teknik kombinasi *chaos map* pada citra berwarna.

1.3. Kontribusi Penelitian

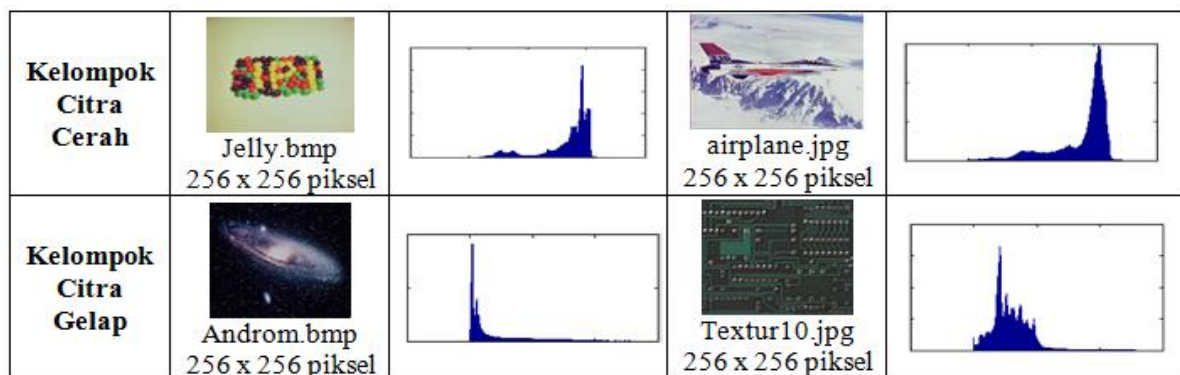
Dengan melakukan analisis yang tepat maka diharapkan dapat menentukan algoritma terbaik untuk teknik enkripsi chaos pada citra berwarna dan penerapan penyandian data pada perangkat bergerak.

Bab 2

Tinjauan Pustaka

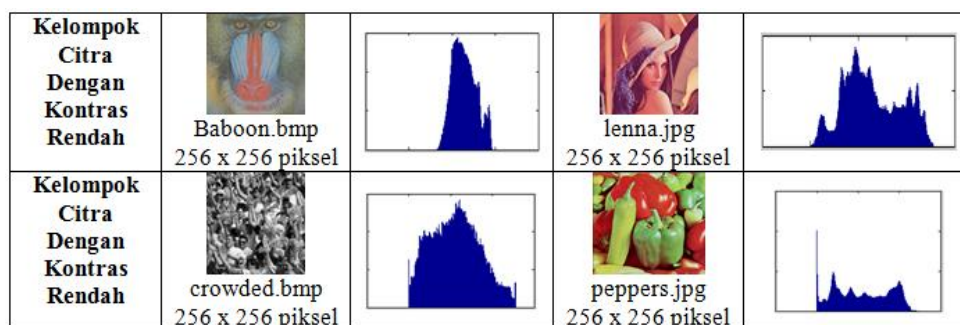
Beberapa kajian hasil penelitian yang berkaitan dengan teknik enkripsi chaos yang telah dilakukan oleh para peneliti akan diulas berikut ini.

Pada penelitian yang dilakukan oleh Naniek Widyastuti dan Emy Setyaningsih (2014) [4], pengujian dilakukan dengan menggunakan citra dengan format .bmp dan .jpg yang dikelompokkan berdasarkan karakteristik tingkat kecerahan, tingkat kontras dan ukuran yang berbeda. Tujuannya adalah untuk mengetahui pengaruh enkripsi pada berbagai karakteristik citra. Kelompok pertama dari citra yang digunakan pada pengujian yaitu berdasarkan tingkat kecerahan citra (brightness), dimana tingkat kecerahan dari suatu citra dapat dilihat dari histogram warna yang mengelompok di salah satu sisi saja seperti terlihat pada gambar 2.1.



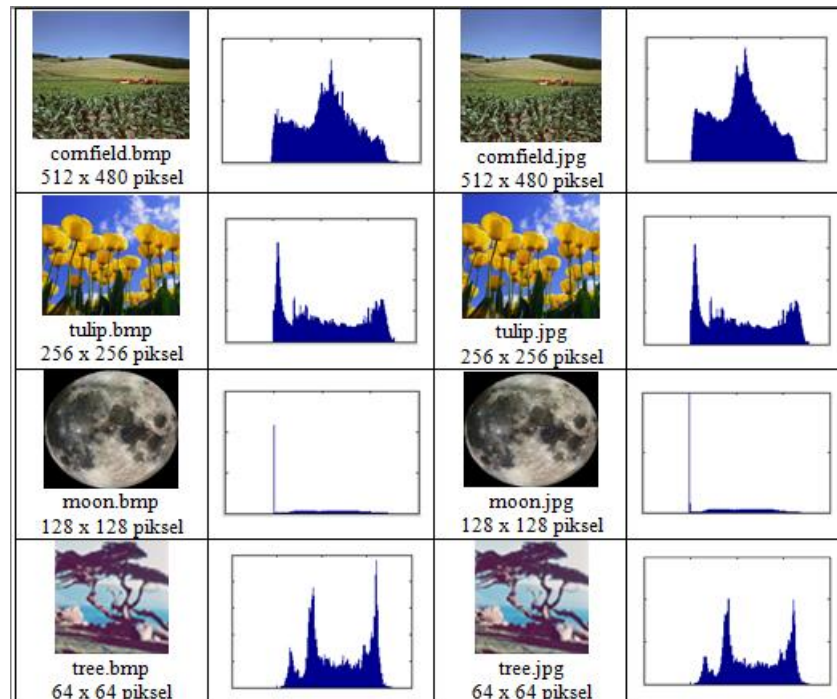
Gambar 2.1. Contoh Citra yang Mewakili Citra Cerah dan Citra Gelap

Kelompok kedua berdasarkan kekontrasan citra (contrast). Tingkat kekontrasan dari suatu citra dapat dilihat dari histogramnya yang menyempit di bagian tengah atau melebar seperti terlihat pada gambar 2.2.



Gambar 2.2. Contoh Citra yang Mewakili Citra Dengan Kontras Rendah






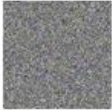










Kelompok ketiga berdasarkan ukuran citra. Citra yang digunakan dalam pengujian ini terdiri dari citra dengan ukuran 512 x 480 piksel, 256 x 256 piksel, 128 x 128 piksel, serta 64 x 64 piksel .seperti terlihat pada Gambar 2.3.



















Gambar 2.3. Contoh Citra yang Mewakili Citra Dengan Berbagai Ukuran

Hasil pengujian kelompok citra maka berdasarkan uji secara visual dapat dilihat pada Tabel 2, Tabel 3 dan Tabel 4. Berdasarkan pengamatan secara visual dari histogram *plain-image* dengan histogram dari *cipher-image* pada Tabel 2.1, Tabel 2.2 dan Tabel 2.3, terlihat histogram *cipher-image* memiliki perbedaan yang cukup signifikan dengan histogram *plain-image*, hal ini menunjukkan distribusi keragaman intensitas warna yang cukup baik. Hasil uji visual pada histogram *cipher-image* terlihat relatif datar baik pada citra dengan format .bmp maupun .jpg, hal ini memperlihatkan bahwa distribusi kemunculan setiap intensitas relatif sama, hal ini menunjukkan bahwa algoritma enkripsi yang digunakan menghasilkan *cipher-image* yang tidak begitu berarti ketika dilakukan *statistical attack* oleh kriptanalis.

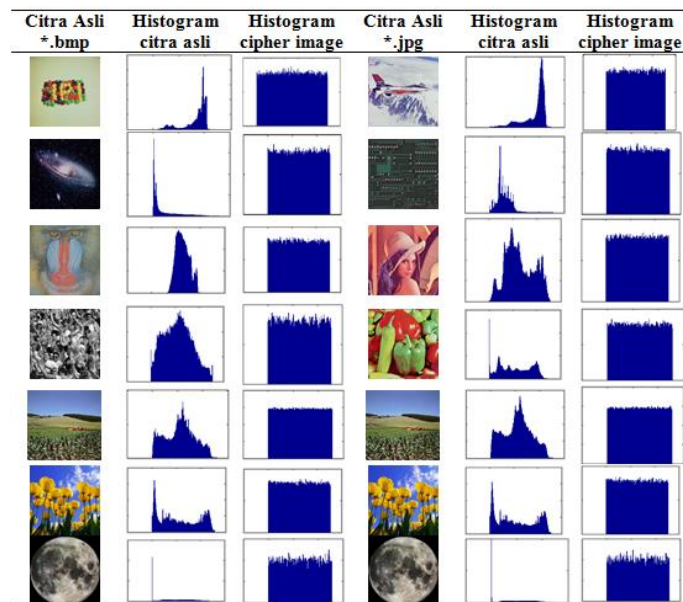
Tabel 2.1. Hasil Uji Visual Citra Berdasarkan Tingkat Kecerahan Dan Kontras Citra

Kelompok citra	Citra Asli *.bmp	Citra Hasil Enkripsi	Citra Asli *.jpg	Citra Hasil Enkripsi
Cerah				
Gelap				
Kontras Rendah				
Kontras Tinggi				

Tabel 2.2. Hasil Uji Visual Citra Berdasarkan Ukuran Piksel

Kelompok Ukuran Piksel	Citra Asli *.bmp	Citra Hasil Enkripsi	Citra Asli *.jpg	Citra Hasil Enkripsi
512 x 480				
256 x 256				
128 x 128				
64 x 64				

Tabel 2.3. Hasil Analisis Histogram



Berdasarkan uji statistik untuk mengukur apakah algoritma enkripsi yang diusulkan cukup aman untuk diimplementasikan, maka dilakukan pengujian menggunakan parameter uji statistik antara lain nilai korelasi, entropi, kualitas enkripsi dan waktu proses enkripsi dan dekripsi. Hasil dari pengujian statistik dapat dilihat pada Tabel 2.4.

Tabel 2.4. Hasil Uji Statistik Citra Berdasarkan Tingkat Kecerahan Dan Kontras

Nama File	Ukuran Piksel	Ukuran File (KB)	Kode Sandi	Hasil Pengukuran Nilai			Waktu Proses (detik)	
				He	Eq	Ic	Enkripsi	Dekripsi
Jelly.bmp	256x256	192	18820	7,9974	30,0371	0,00000423518	1,20121	1,01401
androm.bmp	256x256	192	21020	7,99701	24,8396	-0,00217962	1,07641	0,998406
babonrendah.bmp	256x256	192	05520	7,99713	27,5989	-0,0000411512	1,02961	0,982806
crowded.bmp	256x256	192	24120	7,99722	26,9198	0,000276994	1,07641	1,07641
Rata-rata				7,9972	27,3489	-0,0005	1,09590	27,3489
Aeroplane.jpg	256x256	91,1	02720	7,99746	29,8841	0,000350779	1,12321	1,02961
texture.jpg	256x256	123	21720	7,99703	25,476	-0,000542057	1,04521	0,982806
Lenna.jpg	256x256	95,7	24120	7,99737	27,6958	0,000155785	1,13881	1,04521
peppers.jpg	256x256	104	21520	7,99749	27,4938	0,000198505	1,13881	1,04521
Rata-rata				7,997338	27,63743	0,000040753	1,11151	27,63743

Keterangan :He : *Histogram equalization* (nilai entropi)Eq : *Encryption quality*Ic : *Image correlation*

Rata-rata waktu enkripsi dan dekripsi untuk citra tergantung dengan ukuran citra dimana citra dengan ukuran kecil akan lebih cepat dibandingkan citra dengan ukuran yang lebih besar. Tabel 2.5 juga memperlihatkan bahwa citra dengan ukuran 2 kali lebih besar membutuhkan waktu enkripsi dan dekripsi tiga kali lebih lama.

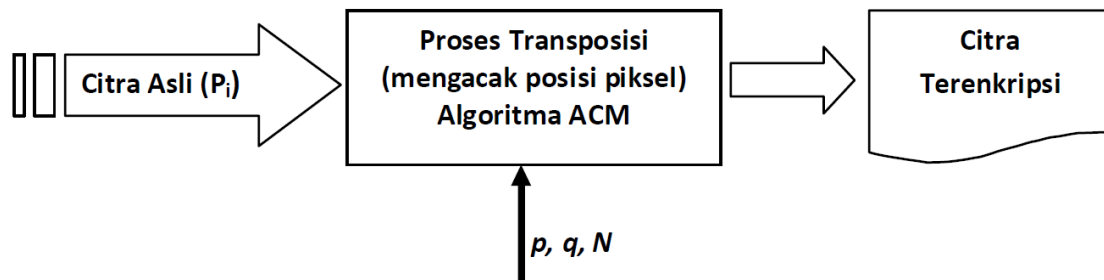
Tabel 2.5. Hasil Uji Statistik Citra Berdasarkan Ukuran Citra

Nama File	Ukuran Piksel	Ukuran File (KB)	Kode Sandi	Hasil Pengukuran Nilai			Waktu Proses (detik)	
				He	Eq	Ic	Enkripsi	Dekripsi
cornfield.bmp	480x512	720	02420	7,99929	26,8417	0,000536007	6,56764	6,39604
tulip.bmp	256x256	192	14320	7,99733	27,0726	0,00134331	1,04521	0,998406
moon.bmp	128x128	48	14120	7,99009	26,3117	-0,00479797	0,296402	0,265202
tree.bmp	64x64	12	21720	7,95791	27,4847	0,000666871	0,109201	0,0624004
cornfield.jpg	480x512	309	02220	7,99926	26,8422	0,000509355	6,42724	6,39604
tulip.jpg	256x256	107	14520	7,99742	27,0718	0,00103276	0,982806	0,998406
moon.jpg	128x128	32,7	14020	7,98876	26,3137	-0,00470688	0,280802	0,249602
tree.jpg	64x64	20,2	21920	7,9534	27,4767	0,0020594	0,093601	0,0624004

Kesimpulan antara lain secara visual citra hasil enkripsi tidak terlihat lagi yang menunjukkan keteracakan warna dan perubahan intensitas warna yang cukup signifikan. Distribusi keragaman intensitas warna yang cukup baik yang ditunjukkan hasil histogram cipher image memiliki perbedaan yang cukup signifikan dengan histogram plain image-nya. Hasil uji visual pada histogram cipher image terlihat relatif datar sehingga algoritma enkripsi yang digunakan tidak dapat memberikan cukup petunjuk untuk dilakukan *statistical attack* oleh kriptanalis. Algoritma enkripsi yang dirancang aman terhadap serangan kriptanalis terlihat dari nilai rata-rata nilai entropinya (He) adalah 7.99 yang mendekati 8, rata-rata nilai korelasi antara plain image dengan cipher image bernilai 0,0003, dan kualitas enkripsi sebesar 27,21 db. Algoritma ini cukup efektif untuk penyandian data citra warna, karena rata-rata waktu proses yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi pada citra dengan ukuran 256x256 piksel rata-rata sekitar 1,06 detik. Untuk citra dengan ukuran 2(dua) kali lebih besar maka waktu yang dibutuhkan 3 kali lipat waktu proses enkripsi maupun dekripsinya.


Menurut Suryadi dkk [8] Chaos adalah tipe perilaku suatu sistem ataupun fungsi yang bersifat acak. Fungsi chaos cocok untuk merancang sarana untuk menunjukkan posisi baru dari piksel [x_1 , y_1], Sedangkan N menunjukkan ukuran citra inputnya berupa citra berbentuk bujursangkar (*square*) yaitu $N \times N$. Teknik algoritma yang digunakan adalah teknik

permutasi dengan menukar posisi piksel-piksel sehingga terkesan acak. Implementasi algoritmanya menggunakan bahasa pemrograman Python. Program aplikasi tersebut diujicobakan terhadap 5 data uji berbeda namun dengan tampilan gambar yang sama.

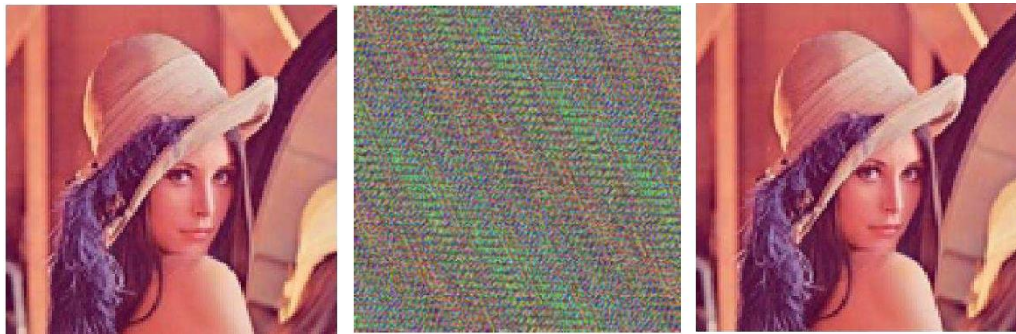


Gambar 2.4. Bentuk Umum Proses Enkripsi Menggunakan Arnold's Cat Map

Tabel 2.6. Citra Data Uji

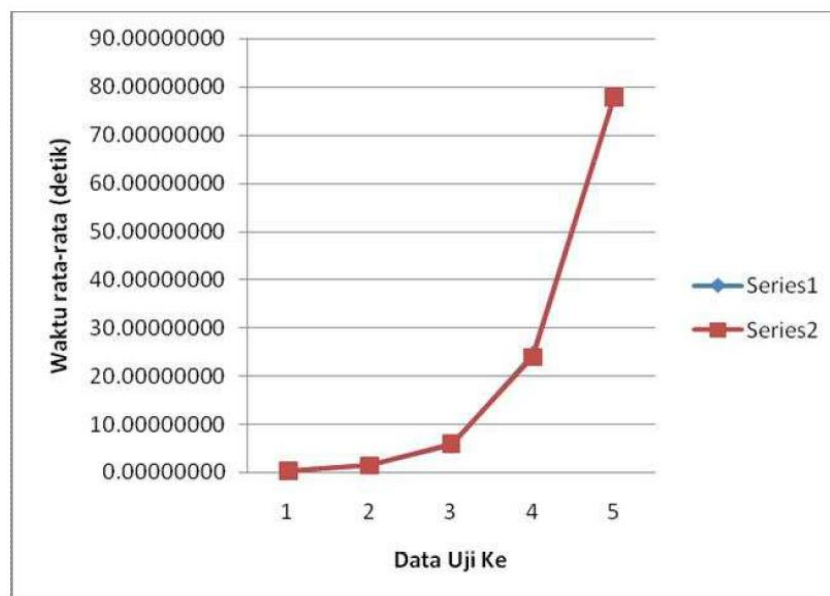
Data Uji ke	Nama File	Tampilan Gambar	Ukuran Citra (piksel)
1.	Lena1 .bmp		128 x 128
2.	Lena2 .bmp		256 x 256
3.	Lena3 .bmp		512 x 512
4.	Lena4 .bmp		1024 x 1024
5.	Lena5 .bmp		2048 x 2048

Proses pengujiannya dilakukan dengan memasukkan nilai parameter kunci p , q dan N . Untuk nilai p dan q nya pada setiap uji coba bernilai sama, dalam hal ini yaitu $p = 157$ dan $q = 37$. Sedangkan nilai N tergantung pada ukuran piksel data uji yang digunakan. Adapun hasil dari enkripsi dan dekripsinya terhadap satu uji coba untuk file Lena1.bmp, tampak pada Gambar 5.



Gambar 2.5. (a) Citra asli, (b) Citra terenkripsi, (c) Citra terdekripsi

Pada gambar 2.6 dan tabel 2.7 dapat dilihat bahwa waktu proses enkripsi dan dekripsi relatif sama. Selain itu, tampak bahwa rata-rata waktu proses enkripsi dan dekripsi berbanding lurus terhadap ukuran piksel citra inputnya. Sehingga, semakin besar ukuran piksel suatu citra maka akan semakin lama rata-rata waktu yang dibutuhkan untuk proses enkripsi dan dekripsinya.



Gambar 2.6. Rata-rata Waktu Enkripsi dan Dekripsi Data Uji Lena.bmp

Tabel 2.7. Rata-rata Waktu Proses Enkripsi dan Dekripsi

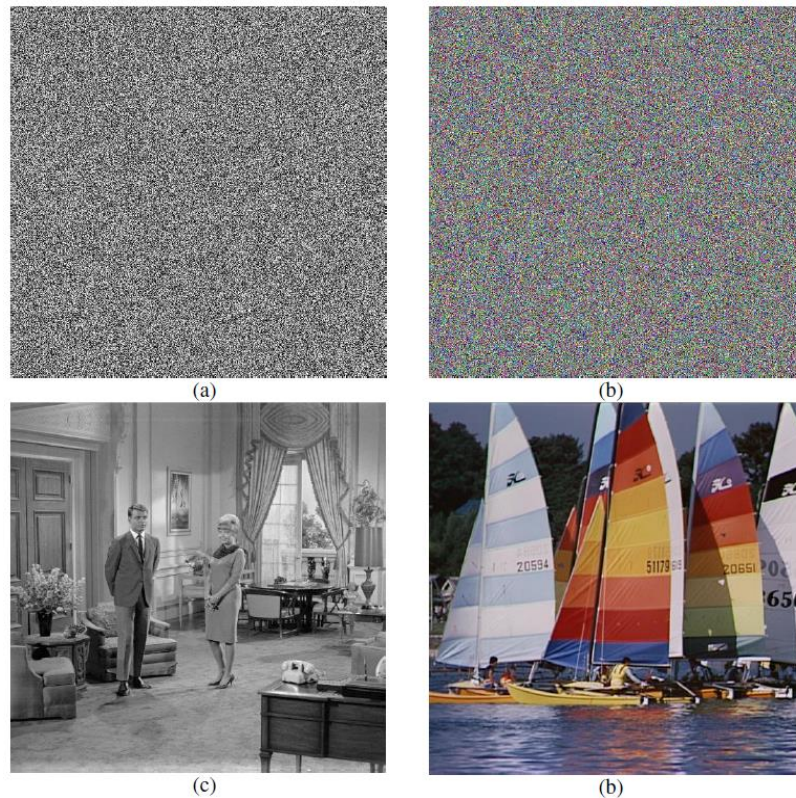
Data Uji Ke-	Nama File	Ukuran Citra (piksel)	Rata-rata Waktu Enkripsi (detik)	Rata-rata Waktu Dekripsi (detik)
1.	Lena1.bmp	128 x 128	0.354699979	0.345399973
2.	Lena2.bmp	256 x 256	1.471900007	1.506399962
3.	Lena3.bmp	512 x 512	5.833900035	5.984700119
4.	Lena4.bmp	1024 x 1024	24.53229999	23.96350004
5.	Lena5.bmp	2048 x 2048	77,89499998	77,97300004

Menurut Rinaldi Munir [6] (2012), Algoritma enkripsi/dekripsi yang telah didekripsikan, disimulasikan dengan menggunakan kaskas Matlab. Eksperimen dilakukan pada dua buah citra uji, masing-masing citra grayscale dan citra berwarna. Kedua buah citra tersebut merupakan citra uji standard di dalam bidang pengolahan citra, yaitu citra ‘couple’ (512 X 512) dan citra ‘yacht’ (512 X 512), seperti ditunjukkan pada Gambar 7(a) dan 7(b). Parameter kunci yang dipakai di dalam eksperimen adalah: $b = 32$, $c = 41$, $r = 3.9728$, $x_0 = 0.3$, dan $m = 5$.



Gambar 2.7. Dua buah citra uji: (a) ‘couple’ (grayscale) (b) ‘yacht’ (berwarna)

Citra hasil enkripsi (*cipher-image*) masing-masing diperlihatkan pada Gambar 8(a) dan 8(b). Citra hasil enkripsi terlihat sudah tidak dapat dikenali lagi dan tampak seperti citra acak. Dekripsi terhadap cipher-image dengan parameter kunci yang sama menghasilkan kembali tepat seperti citra semula (Gambar 8(c) dan 8(d)).



Gambar 2.8. (a) cipher-image dari 'couple'; (b) cipher-image dari 'yacht'; (c) hasil dekripsi citra 'couple'; (d) hasil dekripsi citra 'yacht'

Histogram merupakan salah satu fitur citra yang penting, sebab sebuah histogram memperlihatkan distribusi intensitas piksel-piksel di dalam citra tersebut. Dalam melakukan serangan dengan teknik analisis statistik, penyerang menggunakan histogram untuk menganalisis frekuensi kemunculan intensitas pixel untuk mendeduksi kunci atau piksel-piksel di dalam plain-image. Agar serangan dengan analisis statistik tidak dimungkinkan, maka di dalam enkripsi citra penting untuk menghasilkan histogram *cipher-image* yang tidak memiliki kemiripan secara statistik dengan histogram plain-image. Oleh karena itu, piksel-piksel di dalam cipher-image seharusnya memiliki distribusi yang (relatif) uniform atau ditunjukkan dengan histogram yang terlihat datar (flat).

Melalui simulasi eksperimen, algoritma ini dapat melakukan enkripsi sembarang citra (baik citra grayscale maupun citra berwarna) dengan baik. Citra hasil enkripsi (*cipher-image*) terlihat seperti citra acak dan sudah tidak dapat dikenali lagi. Analisis histogram memperlihatkan piksel-piksel di dalam *cipher-image* mempunyai distribusi uniform, sedangkan analisis korelasi menunjukkan bahwa piksel-piksel di dalam *cipher-image* tidak berkorelasi, sehingga membuat serangan dengan analisis statistik menjadi sulit. Sifat chaos

yang sensitif terhadap perubahan kecil nilai awal telah ditunjukkan dengan melakukan perubahan kecil pada kunci yang menyebabkan citra tidak berhasil didekripsi, sehingga algoritma ini aman dari serangan exhaustive-key search attack.

Menurut Rawat dan Bhandari [9], Steganografi dapat juga digunakan untuk menyandikan pesan rahasia berupa citra berwarna yang dimasukkan ke dalam sebuah citra lainnya sebagai pembungkusnya, yaitu dengan memanipulasi bit pada posisi paling kecil (least significant bit) pada citra pembungkusnya dengan menggantikannya dengan bit dari citra asli yang akan disembunyikan. Di dalam metode ini citra pembungkus adalah citra warna 24 bit yang dipisahkan ke dalam 3 ruang warna yaitu RGB (merah, hijau, dan biru).



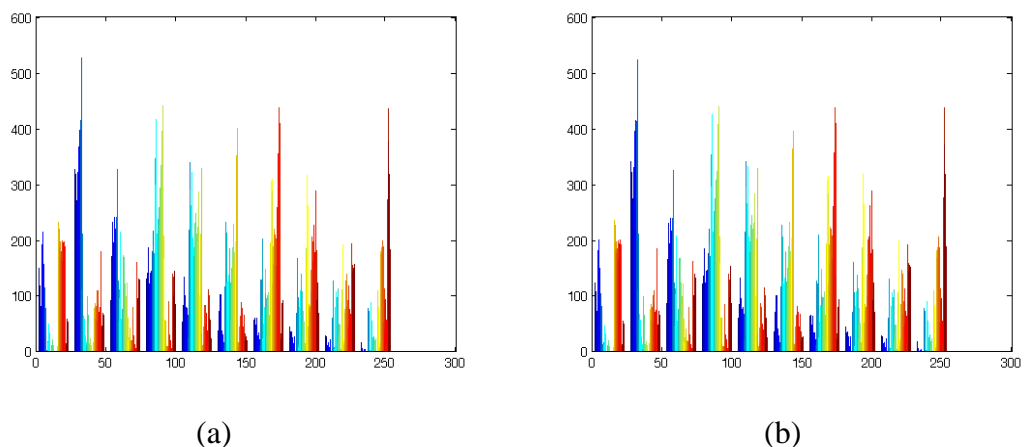
Gambar 2.9. (a) Citra pembungkus; (b) citra warna asli yang akan disembunyikan

Tujuan dari metode ini adalah menyembunyikan citra warna ke dalam citra pembungkus dengan menyembunyikan 1 bit ke dalam ruang warna R, 2 bit ke dalam ruang warna G, dan 3 bit ke dalam ruang warna biru. Hal ini dilakukan untuk meminimalkan kecurigaan atas adanya penyisipan data ke dalam citra pembungkus. Pada piksel pertama dari citra warna yang terdiri dari [11001001], maka proses penyisipan pada piksel pertama citra pembungkus yang terdiri dari [11011100 11000110 10000111] maka piksel pertama dari citra stego adalah [11011101 11000110 100000010]. Citra stego yang dihasilkan dapat terlihat pada gambar 10.



Gambar 2.10. Citra stego yang dihasilkan dengan menyisipkan citra warna asli ke dalam citra pembungkus

Analisis histogram seperti yang terlihat pada gambar 11, yaitu dengan cara membandingkan histogram citra sampul dengan semua citra stego cukup jelas bahwa histogram citra stego berwarna 24 bit hampir mirip dengan citra pembungkus. yaitu hampir tidak ada perubahan atau hampir tidak ada perubahan dalam intensitas warna.



Gambar 2.11. (a) Histogram citra pembungkus; (b) Histogram citra stego

Rangkuman keterbatasan yang terdapat dari tiga tinjauan penelitian di atas adalah sebagai berikut :

1. Keterbatasan yang terdapat pada penelitian Naniek Widyastuti dkk (2014) [4] adalah belum dapat diketahui untuk penerapan citra dengan ukuran lebih besar dari

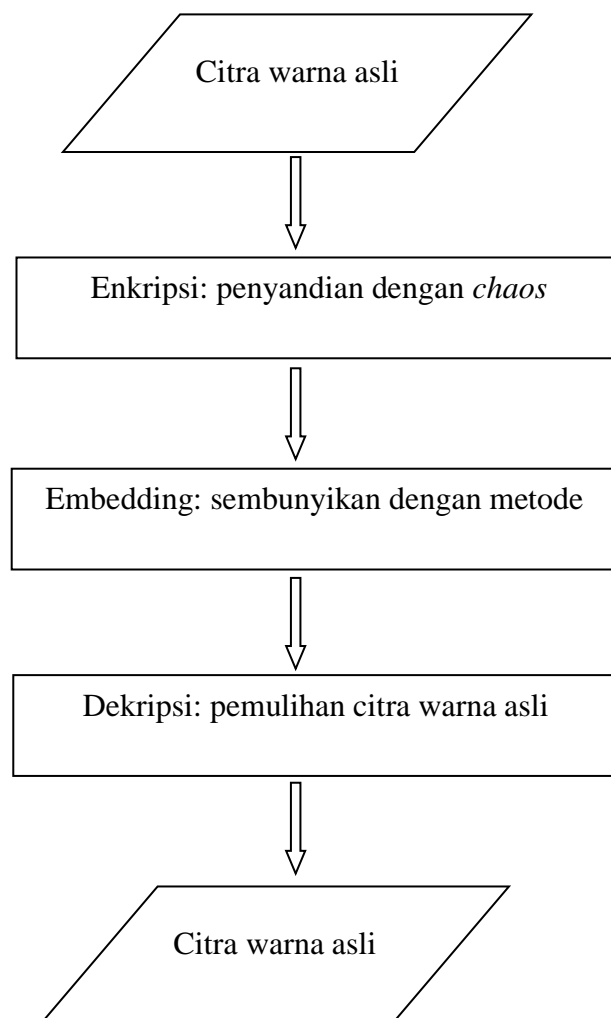
256x256 piksel, dan juga memerlukan waktu yang lama untuk citra berukuran lebih besar.

2. Keterbatasan pada penelitian Suryadi dkk (2014) [8] adalah waktu yang lama untuk citra berukuran besar.
3. Keterbatasan pada penelitian Rinaldi Munir (2012) [7] adalah belum diketahuinya penerapan untuk citra dengan ukuran lebih dari 512 x 512 piksel dan juga belum diketahuinya waktu proses yang dibutuhkan untuk proses enkripsi dan dekripsi.
4. Keterbatasan pada penelitian Rawat dan Bhandari (2013) [9] adalah belum diketahuinya waktu proses untuk penyembunyian citra warna dan ekstraksi citra warna pada berbagai ukuran.

Bab 3

Metodologi

Berdasarkan keterbatasan yang tersaji dari tiga kajian penelitian yang sudah diceritakan sebelumnya, dapat dinyatakan bahwa untuk membuat analisis algoritma menjadi suatu permasalahan tersendiri. Oleh karena itu diperlukan pengembangan metode analisis aplikasi algoritma chaos pada citra. Proposal ini mengusulkan pengembangan metode yang digambarkan pada diagram alur penelitian pada gambar di bawah ini.



Gambar 3.1. Diagram alur penelitian

Agar hasil enkripsi tahan terhadap serangan maka akan dilakukan beberapa analisis terhadap algoritma yang ditemukan , yaitu dengan:

1. Analisis Ruang Kunci (Sensitivitas)
2. Analisis Kualitas Citra
3. Analisis Uniform (Histogram)
4. Analisis waktu untuk citra warna yang berukuran besar.
5. Analisis kemungkinan untuk menyembunyikan citra terenkripsi ke dalam citra berwarna lainnya.

Perkiraan waktu dalam menyelesaikan penelitian ini dapat dilihat pada tabel berikut ini.

Tabel 3.1. Jadwal Rencana Penelitian

Langkah-langkah Penelitian	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Pengumpulan data															
Menguji coba metode yang sudah ada															
Mengevaluasi masing-masing metode yang sudah ada															
Merancang metode pengembangan															
Menguji coba metode pengembangan															
Implementasi metode yang dikembangkan pada data citra warna															
Melakukan evaluasi metode yang dikembangkan															

DAFTAR PUSTAKA

- [1] Dony Ariyus, *Computer Security*, Yogyakarta, Indonesia: Penerbit ANDI, 2006.
- [2] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
- [3] S. R. M. Prasanna, Y. V. S. Rao, and A. Mitra, "An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images," International Journal of Electrical and Computer Engineering, vol. 1, no. 2, 2006.
- [4] Naniek Widyastuti, Emy Setyaningsih, "Implementasi Pengembangan Kunci Chaos Pada Algoritma RC4 Serta Keamanannya Menggunakan Teknik Invisible Watermark", Prosiding SNASTI, 2014
- [5] Naniek Widyastuti, "Pengembangan Metode Beaufort Cipher Menggunakan Pembangkit Kunci Chaos", Jurnal Teknologi Volume 7 Nomor 1, Juni 2014, 73-82.
- [6] Suryadi MT, Zuherman Rustam, Wiwit Widhianto, "Implementasi Algoritma Enkripsi Citra Digital Menggunakan Skema Transposisi Berbasis Fungsi Chaos", Prosiding KOMMIT, 2014
- [7] Rinaldi Munir, "Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi dan Teknik Substitusi menggunakan Arnold Cat Map dan Logistiz Map", SENAPATI, 2012
- [8] Rinaldi Munir, "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif", JUTI, 2012
- [9] Deepesh Rawat and Vijaya Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, PP 15-19, February 2013.
- [10] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Applications 2, PP 102-108, February 2011.
- [11] Debasish Jena, Sanjay Kumar Jena, "A Novel Visual Cryptography Scheme", International Conference on Advanced Computer Control, 2009.
- [12] Hyoung Joong Kim, Vasiliy Sachnev, Su-Jeong Choi, Shijun Xiang, "An Innocuous Visual Cryptography Scheme", Eight International Workshop on Image Analysis for Multimedia Interactive Services(WIAMIS'07),0-7695-2818-X/07 \$20.00 © 2007 IEEE.

- [13] Kiran Kumari, Shalini Bhatia, *Multi-pixel Visual Cryptography for color images with Meaningful Shares*, International Journal of Engineering Science and Technology Vol. 2(6), 2010, 2398-2407.
- [14] Moni Naor & Adi Shamir, *Visual Cryptography*, Springer-Verlag, 1998.
- [15] Reeta Mishra and Aniruddha Bhattacharjya, “*An Exploratory Study on Steganography*”, VSRD International Journal of Computer Science & Information Technology Vol 1(4), PP 189-198, 2011.
- [16] Rupinder Kaur, Mandeep Kaur, Rahul Malhotra, “*A New Efficient Approach towards Steganography*”, International Journal of Computer Science and Information Technologies Vol 2 (2), PP 673-676, 2011.
- [17] Rajkumar Yadav, “*Study of Information Hiding Techniques and their Counterattacks: A Review Article*”, International Journal of Computer Science & Communication Networks Vol. 1 (2), PP 142-164, Oct-Nov 2011.
- [18] Rosziati Ibarahim and Teoh Suk Kuan, *Steganography Imaging System (SIS): Hiding Secret Message inside an Image*, Proceedings of the World Congress on Engineering and Computer Science Vol I, October 2010.