Jurnal Rekayasa Elektrika

VOLUME 10 NOMOR 3 APRIL 2013

JRE	Vol. 10	No. 3	Hal 115–159	Banda Aceh, April 2013	ISSN. 1412-4785 e-ISSN. 2252-620x

Penerapan CIELab dan Chaos sebagai Cipher pada Aplikasi Kriptografi Citra Digital

Linna Oktaviana Sari
Jurusan Teknik Elektro, Fakultas Teknik, Universitas Riau
Kampus Bina Widya KM 12,5 Simpang Baru, Pekanbaru 28293
e-mail: linna.osari@gmail.com

***Abstrak*—Perkembangan jaringan Internet mendukung masyarakat untuk dapat mengirimkan informasi baik teks, citra dan media lainnya dengan cepat. Namun, informasi terutama citra digtal yang dikirimkan melalui internet sangat rentan terhadap serangan, seperti modifikasi dan duplikasi oleh pihak yang tidak berhak. Oleh karena itu telah dikembangkan cabang ilmu yang mempelajari tentang cara-cara pengamanan data salah satunya adalah kriptografi. Penelitian ini mengusulkan kombinasi struktur warna CIELab dan pengacakan kunci dengan persamaan logistik dari *chaos* sebagai cipher baru pada aplikasi kriptografi citra digital. Cipher ini diterapkan pada proses enkripsi dan dekripsi. Aplikasi kriptografi citra digital untuk menerapkan cipher dibangun dengan Matlab R2010a. Berdasarkan hasil penelitian yang telah dilakukan maka diperoleh bahwa CIELab dan *chaos* dapat diterapkan sebagai cipher pada proses enkripsi dan dekripsi untuk aplikasi kriptografi citra digital dengan waktu proses kurang dari 1 detik. Dengan kemungkinan rentang kunci maksimum pada citra RGB sebesar 5,2 x 1033, cipher cukup aman terhadap serangan *brute-force attack*. Citra hasil dekripsi berkualitas baik dengan PSNR lebih besar dari 50 dB untuk format citra digital "tiff" dan "png".**

Kata kunci: ***citra, kriptografi, cipher, CIELab, chaos***

***Abstract*—The development of Internet supports people to transmit information, such as text, images and other media quickly. However, digital images transmitted over the Internet are very vulnerable to attacks, for examples modification and duplication by unauthorized people. Therefore, cryptography as one of method for data security has been developed. This research proposed a combination of color structure CIELab and key randomization by logistic map from chaos as new cipher in digital image cryptographic applications. Cipher is applied to the encryption and decryption process. Implementation of new cipher in cryptographic digital images application was built with Matlab R2010a. Based on the research that has been done, it was found that combination CIELab and chaos can be applied as a new cipher on the encryption and decryption of digital images for cryptographic applications with processing time less than 1 second. Under possible maximum key range on RGB image by 5,2x 1033, the cipher was sufficiently secure against brute-force attack. Decrypted image has good quality with PSNR greater than 50 dB for digital image formatted in "tiff" and "png".**

Keywords: ***image, cryptography, cipher, CIELab, chaos***

I. PENDAHULUAN

Seiring dengan pesatnya perkembangan jaringan komunikasi dan kemajuan teknologi di bidang komputer memungkinkan ribuan orang dapat berkomunikasi dan saling bertukar informasi jarak jauh dalam dunia maya. Pertukaran informasi melalui dunia maya dikenal dengan *cyberspace* atau istilah awam Internet [1]. Dalam dunia maya ini, hampir segala jenis informasi dapat diperoleh, yang dibutuhkan hanyalah sebuah komputer yang terhubung dengan dunia maya. Informasi yang diperoleh dalam dunia maya dapat disajikan dalam berbagai format seperti: teks, citra, audio, maupun video.

Saat ini penggunaan kartu kredit, kartu ATM, telepon seluler, internet, *e-commerce*, *e-government*, *on-line banking* dan lain-lain telah menjadi kebutuhan sehari-hari yang selalu hadir karena kemajuan teknologi informasi dan komunikasi. Perangkat-perangkat teknologi tersebut dalam operasionalnya melibatkan data atau informasi baik yang ditransfer maupun yang disimpan.

Di dalam dunia maya ini ribuan orang akan saling bertukar pesan digital baik berupa teks, citra, maupun video melalui perangkat digital. Begitu banyaknya pengguna teknologi ini, baik perusahaan, lembaga negara, lembaga keuangan, department pertahanan atau militer, bahkan individu-individu yang tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau pesaingnya atau negara lain.

Seiring dengan kemajuan teknologi tersebut, ancaman-ancaman terhadap informasi seperti modifikasi dan duplikasi menyebabkan dibutuhkannya keamanan informasi. Nilai informasi yang digunakan dalam transaksi on-line tersebut sangatlah vital, sehingga memerlukan penanganan yang serius dalam pengamanan informasinya.

Pengamanan informasi tersebut sangat dibutuhkan untuk menjaga privasi (*confidentiality*) informasi,

memastikan identitas atau otentikasi (*authentication*), menjaga keutuhan atau integritas (*integrity*) informasi, dan menjamin ketersediaan (*availability*) [2].

Oleh karena itu dibutuhkan sistem pengamanan data yang sesuai dengan perkembangan teknologi sehingga data yang dikirimkan melalui jaringan tidak jatuh pada orang yang tidak berhak dan tidak dimodifikasi. Untuk itu telah dikembangkan dalam bidang teknologi informasi cabang ilmu yang mempelajari tentang cara-cara pengamanan data, yaitu kriptografi, steganografi, dan watermarking [3].

Kriptografi adalah suatu seni untuk menyembunyikan informasi dari sebuah pesan, sehingga pesan tersebut terlihat tidak memiliki arti [3]. Maraknya pemberitaan tentang penyadapan ikut mempopulerkan kriptografi kepada masyarakat Indonesia. Walaupun kriptografi bukanlah hal baru, tetapi untuk masyarakat Indonesia kriptografi masih jarang sekali dibicarakan secara umum.

II. Latar Belakang

Kriptografi tidak hanya dilakukan pada data yang berupa teks (pesan), melainkan juga berupa gambar (citra). Di antara jenis-jenis digital media yang ada, citra atau gambar adalah yang paling rentan terhadap operasi-operasi illegal berupa duplikasi, modifikasi, dan pemalsuan, karena data berupa citra dapat dengan mudah ditangkap oleh mata manusia. Sehingga banyak citra digital menjadi informasi yang sangat penting untuk diamankan dan dijaga kerahasiannya agar tidak diakses oleh orang yang tidak berhak dan diubah kebenaran isi informasi dari citra digital tersebut, sebagai contoh foto digital, sertifikat digital, tanda tangan digital (*digital signature*), dan lain sebagainya.

Hal tersebut menyebabkan kebutuhan akan program-program aplikasi kriptografi yang dapat membantu pemakai untuk menjamin keamanan data berupa citra digital pada saat ditransmisikan juga semakin besar. Untuk menjamin keamanan data berupa citra digital yang ditransmisikan, maka citra digital dienkripsi dengan *cipher* enkripsi (algoritma enkripsi) menjadi *cipher image* atau gambar yang tidak memiliki arti. Setelah sampai di tujuan, maka *cipher image* didekripsikan kembali dengan *cipher* dekripsi menjadi citra yang serupa dengan citra asli (*decipher image*) yang diterima oleh penerima.

Namun, tidak semua *cipher* enkripsi maupun dekripsi untuk teks dapat diterapkan pada enkripsi dan dekripsi citra digital dikarenakan perbedaan karakteristik teks dan citra digital, kesulitan implementasi dan proses yang lambat. Hal tersebut dapat diatasi dengan menerapkan *cipher* enkripsi dan dekripsi yang sesuai dengan karakteristik untuk citra digital.

Hasil telusuran penelitian terdahulu yang berkaitan dengan penemuan *cipher* citra untuk enkripsi dan dekripsi pada kriptografi citra digital telah banyak dikembangkan. Pada tahun 1998, dikembangkan juga *chaotic Kolmogrov-flowbased image encryption technique*, dimana citra dianggap sebagai suatu blok tunggal dan dipermutasikan melalui pengendalian sistem kunci *chaotic* [4]. Pada tahun 1999, Yen dan Guo mengembangkan metode enkripsi yang disebut BRIE, berdasarkan *logistic map* dimana kunci rahasia terdiri dari dua integer dan kondisi awal pemetaan logistik [5]. Pada tahun 2001, juga telah dikembangkan teknik kriptogarafi citra menggunakan teknik kompresi citra dan vektor kuantisasi untuk merancang sistem kripto yang efisien [6]. Prasanna dkk. juga telah mengembangkan *cipher* untuk enkripsi citra dengan manipulasi magnitude dan fase dengan menggunakan kunci citra pembawa [3]. M.A.B. Younes melakukan penelitian yang menghasilkan *cipher* citra hasil dari transformasi berdasarkan blok dan algoritma Blowfish [7]. Pada Tahun 2008, dihasilkan algoritma enkripsi selektif sebagai lawan dari enkripsi total [8] yang bertujuan untuk meminimalkan proses komputasi. Pada [9] diterapkan teknik permutasi dan scrambling pada enkripsi citra untuk domain frekuensi sehingga meningkatkan kompleksitas komputasi terhadap serangan *chose plaintext*. Pada tahun 2010, dilakukan penelitian yang menghasilkan *cipher* untuk enkripsi citra dengan peta *chaotic* dan transformasi Gyrator [10].

Pada tahun 2011 telah dilakukan penelitian yang menghasilkan *cipher* dengan index baru pada sistem *chaotic*, kemudian permutasi dilakukan pada *pixel* dari citra skala keabuan pada basis posisi indeks dari urutan *chaotic* [11]. Pada tahun 2012, dihasilkan *cipher* tranformasi wavelet untuk mengkomposisikan dan mengkorelasikan kembali citra menjadi komponen yang detil, hasilnya dienkripsi dengan kunci *chaos* [12]. Pada tahun 2012 dilakukan penelitian dengan menerapkan transformasi FFT dan *chaos* sebagai *cipher* pada perangkat lunak kriptografi citra digital [13].

Struktur warna telah banyak dikembangkan, salah satunya CIElab. CIELab adalah salah satu struktur warna yang didefinisikan *Commicion International de 1'Eclairage/The International Commission on Illumination* (CIE) pada tahun 1976 (CIE 1976 L*a*b*) [14]. CIElab telah banyak digunakan dalam aplikasi teknik dan aplikasi citra warna [15]. Pada tahun 2010, dilakukan penerapan CIElab pada proses segmentasi dan deteksi tepi [16].

Berdasarkan studi literatur yang telah dilakukan, maka pada penelitian ini dilakukan inovasi *cipher* baru sebagai *cipher* enkripsi dan dekripsi yang diterapkan pada aplikasi kriptografi citra digital. *Cipher* ini dihasilkan dengan cara mengkombinasikan ruang atau struktur warna CIELab dan pengacakan *chaos* pada citra digital. *Cipher* diterapkan pada proses enkripsi untuk menghasilkan *cipher image* dan proses dekripsi untuk mengembalikan citra digital asli.

Pada penelitian ini *cipher* enkripsi dan dekripsi dihasilkan dengan mengkombinasikan ruang warna CIELab pada citra digital dengan suatu kunci yang dihasilkan dari pengacakan citra digital menggunakan *chaos*.

A. Strukutr Warna CIELab

CIELab adalah salah satu struktur warna yang didefinisikan CIE. Pada CIELab, besaran CIE_L* untuk

mendeskripsikan kecerahan warna, 0 untuk hitam dan L* = 100 untuk putih. Dimensi CIE_a* mendeskripsikan jenis warna hijau – merah, dimana angka negatif a* mengindikasikan warna hijau dan sebaliknya CIE_a* positif mengindikasikan warna merah. Dimensi CIE_b* untuk jenis warna biru – kuning, dimana angka negatif b* mengindikasikan warna biru dan sebaliknya CIE_b* positif mengindikasikan warna kuning. Transformasi RGB (R*ed, Green, Blue*) – CIELab dapat dilakukan dengan (1) berikut [14]:

$$X = CR$$

dimana

$$C = C'^{G}$$

$C = R, G, B$ dan $G = 2.2$,

$$X_1 = X / X_n$$
$$Y_1 = Y / Y_n$$
$$Z_1 = Z / Z_n$$

$$X_1 = \begin{cases} X_1^{1/3} \text{ jika } X_1 > 0.008856 \\ 7.787 X_1 + \dfrac{16}{116} \end{cases}$$

$$Y_1 = \begin{cases} Y_1^{1/3} \text{ jika } Y_1 > 0.008856 \\ 7.787 Y_1 + \dfrac{16}{116} \end{cases}$$

$$Z_1 = \begin{cases} Z_1^{1/3} \text{ jika } Z_1 > 0.008856 \\ 7.787 Z_1 + \dfrac{16}{116} \end{cases}$$

sehingga L*a*b menjadi:

$$L^* = 116 Y_1 - 16$$
$$a^* = 500\left(X_1 - Y_1\right)$$
$$b^* = 200\left(Y_1 - Z_1\right). \quad (1)$$

Sedangkan tranformasi dari CIELab – RGB dapat dilakukan dengan (2):

$$Y_1 = \frac{L^* + 16}{116}$$

$$X_1 = \frac{a^*}{500} + Y_1$$

$$Z_1 = -\frac{b^*}{200} + Y_1$$

$$X_1 = \begin{cases} X_1^3 \text{ jika } X_1 > 0.206893 \\ (X_1 - \dfrac{16}{116}) / 7.787 \end{cases}$$

$$Y_1 = \begin{cases} Y_1^3 \text{ jika } Y_1 > 0.206893 \\ (Y_1 - \dfrac{16}{116}) / 7.787 \end{cases}$$

$$Z_1 = \begin{cases} Z_1^3 \text{ jika } Z_1 > 0.008856 \\ (Z_1 - \dfrac{16}{116}) / 7.787 \end{cases}$$

$$X = X_n X_1$$
$$Y = Y_n Y_1$$
$$Z = Z_n Z_1$$
$$R = C^{-1} X. \quad (2)$$

B. *Logistik Map*

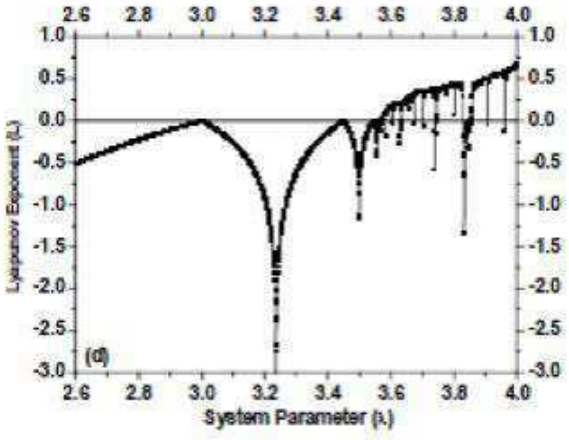
Kunci yang digunakan pada proses enkripsi dan dekripsi, menggunakan kunci *chaos* berupa persamaan *logistic map*. Persamaan Logistik (*Logistic Map*) adalah salah satu bentuk yang paling sederhana dari proses *chaos*. [17] menunjukkan bahwa model sederhana ini menunjukkan perilaku yang kompleks. Karena kesederhanaan matematisnya, model ini terus memunculkan ide-ide baru dalam teori *chaos* serta aplikasi kekacauan dalam kriptografi. Berikut adalah persamaan dari peta logistik [17]:

$$Xn+1 = \lambda\, Xn\, (1 - Xn) \quad (3)$$

dimana Xn adalah *variabel state*, yang terletak di interval [0,1] dan λ disebut sebagai parameter sistem yang dapat memiliki nilai antara 1 dan 4. Pada dasarnya, peta ini, seperti peta satu-dimensi lainnya, yaitu aturan untuk mendapatkan sebuah bilangan dari bilangan lain..

Pada Gambar 1 dapat dilihat bahwa persamaan yang menghasilkan sifat *chaos* terbesar adalah saat λ bernilai sekitar 4. *Logistic Map* tidak akan bersifat *chaos* saat λ bernilai < 3.559 yang menghasilkan nilai Lypunof negatif. Menurut perhitungan yang telah dilakukan, dapat disimpulkan bahwa *logistic map* memberikan karakter *chaos* terbaik saat λ bernilai sangat dekat dengan 4 [15].

Persamaan logistik ini dapat diterapkan dalam



Gambar 1. Perilaku dari Logistic Map: Lyapunov exponent (pengukuran kuantiatif dari sifat chaos) sebagai fungsi dari parameter λ

kriptografi dengan membuat fungsi seperti yang telah dicantumkan diatas. Setelah membuat fungsi tersebut, dilakukan proses perhitungan dengan melakukan iterasi secara berulang, sehingga akan selalu mendapatkan bilangan yang acak.

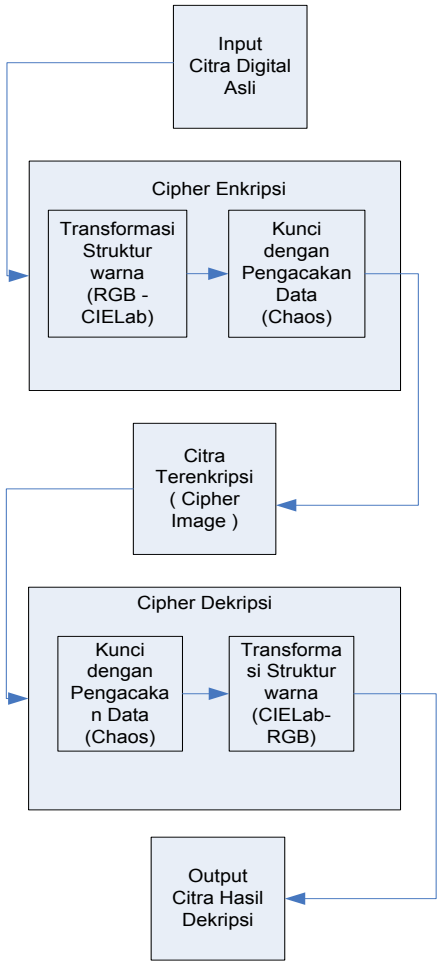
III. METODE

A. *Proses Enkripsi dan Dekripsi*

Pada penelitian ini dihasilkan *cipher* baru untuk proses enkripsi dan dekripisi. Pada Gambar 2, dapat dilihat blok diagram penerapan *cipher* baru pada proses enkripsi dan dekripsi yang diusulkan. *Cipher* yang dihasilkan dengan mengkombinasikan transformasi struktur warna citra digital dari ruang warna RGB (*Red Green Blue*) menjadi ruang warna CIELab dengan kunci yang dihasilkan dari pengacakan citra digital menggunakan persamaan logistik *chaos*.

Cipher enkripsi dan dekripsi diterapkan pada aplikasi kriptografi citra digital. Pada blok *cipher* enkripsi terdapat tahapan, yaitu

1. Transformasi struktur warna RGB ke CIELab. Citra Asli akan ditransformasikan struktur warnanya dari RGB menjadi CIELab dengan menggunakan (1). RGB adalah struktur warna tiga dimensi yang dipakai sebagai struktur warna *truecolor* pada citra digital, dimana R(*Red*) menyatakan merah, G(*Green*) menyatakan Hijau dan B(*Blue*) menyatakan biru. Sedangkan CIELab (L*a*b) adalah struktur warna citra yang menyatakan L sebagai pencahayaan, dan a menyatakan merah atau hijau dan b menyatakan kuning atau biru. Transformasi ini menghasilkan Citra yang sudah berbeda struktur warna dari citra asli.
2. Proses penguncian (*lock*) dengan kunci hasil pengacakan citra digital menggunakan *chaos* pada (3). Hasil transformasi dari tahapan satu dilakukan pengacakan pada citra digital pada setiap komponen L,*a, dan*b dengan kunci hasil pengacakan citra digital menggunakan *chaos* pada (3). Kondisi ini tentunya akan menyulitkan *hacker* untuk menemukan citra asli.



Gambar 2. Blok diagram *cipher* citra digital pada proses enkripsi dan dekripsi.

Keluaran dari blok *cipher* enkripsi merupakan citra digital yang tidak dipahami. Citra digital inilah yang nantinya dikirimkan melalui jaringan.

Citra digital yang terenkripsi di bagian penerima, harus didekripsi untuk mendapatkan citra digital asli untuk dipahami oleh penerima yang berhak. Di bagian penerima, citra digital yang terenkripsi masuk ke dalam blok *cipher* dekripsi. Pada blok *cipher* dekripsi terdapat tahapan berikut , yaitu

1. Proses pembukaan (*unlock*) dengan kunci hasil pengacakan pada citra terenkripsi dengan *chaos* pada (3). Setelah kunci dihasilkan, citra digital masih berada pada struktur warna CIElab.
2. Transformasi struktur warna dari CIELab ke RGB pada (2). Citra yang telah dibuka kuncinya, ditransformasikan struktur warnanya dari CIELab ke RGB sehingga diperoleh citra digital asli.

B. *Usulan Cipher Baru untuk Enkripsi dan Dekripsi*

Secara garis besar algoritma enkripsi dapat dijabarkan sebagai berikut :

1. Masukan berupa citra digital RGB ukuran m x n x p.
2. Transformasikan citra digital struktur R,G,B menjadi citra digital struktur L,*a, *b dengan (1).
3. Proses perhitungan kunci dengan (3) dengan melakukan iterasi secara berulang sebanyak (m x n), sehingga akan selalu mendapatkan bilangan yang acak.
4. Konversikan kunci dari *real* ke *integer* dengan menggunakan menggunakan fungsi uint8 pada matlab.
5. Terapkan kunci pada citra digital struktur L,*a, *b untuk pengacakan dengan melakukan XOR (*exclusive* OR).

Sedangkan algoritma deskripsi secara garis besar dapat dijabarkan sebagai berikut :

1. Masukan berupa citra digital L,*a, *b yang terenkripsi.
2. Proses perhitungan kunci dengan (3) dengan melakukan iterasi secara berulang sebanyak (m x n), sehingga akan selalu mendapatkan bilangan yang acak.

3. Konversikan kunci dari riil ke integer uint8 dari matlab.
4. Terapkan kunci pada citra digital dengan melakukan XOR (*exclusive* OR).
5. Transformasikan citra digital struktur L,*a, *b menjadi citra digital struktur R,G,B dengan (2).

Cipher enkripsi dan *cipher* dekripsi yang telah dihasilkan diterapkan pada aplikasi kriptografi citra digital dengan menggunakan Matlab R2010a.

IV. Hasil dan Pembahasan

Pada bagian ini terdapat beberapa hasil dan analisa yang akan dilakukan yaitu :

1. Hasil dan analisa penerapan *cipher* pada proses enkripsi dan dekripsi citra digital.
2. Hasil dan analisa *cipher* terhadap format citra digital berbeda.
3. Hasil dan analisa *cipher* pada ukuran citra berbeda terhadap waktu proses .
4. Analisa histogram citra digital.
5. Pengujian dan Analisa Kekuatan *Cipher*

Pada Tabel 1 berikut terdapat beberapa parameter yang digunakan dalam pengujian dan analisa *cipher* untuk diterapkan pada proses enkripsi dan dekripsi pada aplikasi kriptografi citra digital. Aplikasi kriptografi citra digital dibangun dengan Matlab R2010a.

A. Hasil dan Analisa Penerapan Cipher pada Proses Enkripsi dan Dekripsi Citra Digital.

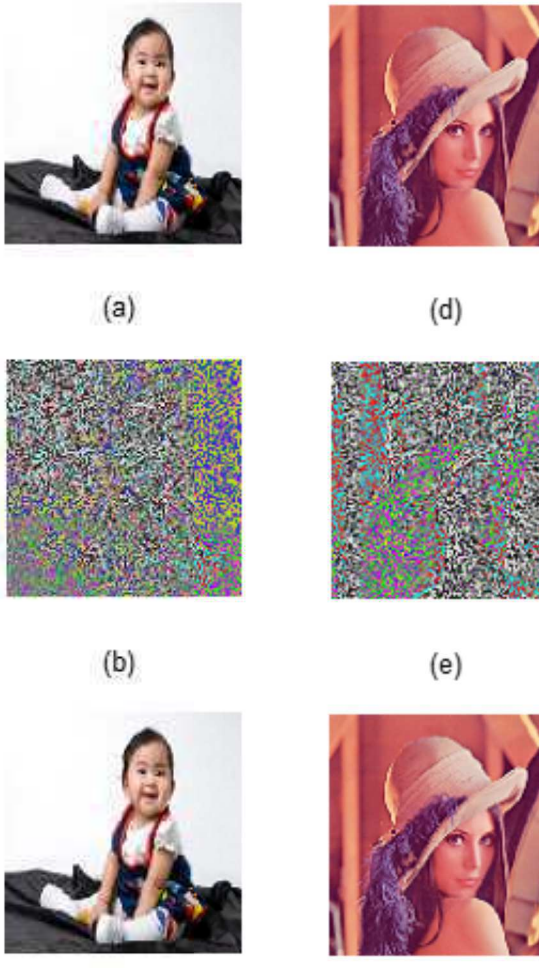
Pada bagian ini, dilakukan pengujian untuk melihat secara visual hasil penerapan *cipher* pada enkripsi dan dekripsi pada citra digital. Pada Gambar 3 dapat dilihat hasil penerapan *cipher* pada proses enkripsi dan dekripsi pada citra digital “mynadia.jpg” dan “lena.jpg”. Gambar 3 (a) dan (d), merupakan citra asli yang akan dienkripsi dengan *cipher* enkripsi. Gambar 3(b) dan (e) merupakan hasil dari proses enkripsi citra digital yang terenkripsi dari *cipher* enkripsi baru yang dihasilkan.

Pada gambar tersebut tampak secara visual bahwa citra digital yang terenkripsi tak dapat dipahami isi informasinya. Hal ini menunjukkan bahwa *cipher* enkripsi baru yang dihasilkan dapat atau berhasil melakukan proses enkripsi pada citra digital. Sedangkan Gambar 3(c) dan (f) merupakan citra hasil dekripsi dari citra terenkripsi menggunakan *cipher* dekripsi baru. Pada gambar tersebut tampak secara visual bahwa citra dekripsi yang dihasilkan seperti citra aslinya.

Hal ini menunjukkan bahwa *cipher* dekripsi baru yang dihasilkan dapat atau berhasil melakukan proses dekripsi sehingga dapat mengembalikan citra asli. Secara keseluruhan *cipher* enkripsi dan dekripsi baru yang dihasilkan dapat melakukan proses enkripsi dan dekripsi pada citra digital.

Tabel 1. Parameter untuk pengujian cipher

No	Parameter	Nilai Parameter
1.	Parameter System Logistik (λ)	λ=3.998
2.	Input citra 1	
	“mynadia.jpg”	Dimensi(m x n x p) = 256x256x3 uint 8,
	“lena.jpg”	Ukuran file =10KB Dimensi = 256x256x3 uint 8, Ukuran file = 20KB
3.	Input citra 2	
	“mynadia.png”	Dimensi = 256x256x3uint8, Ukuran file =63KB
	“lena.png”	Dimensi = 256x256x3 unti8, Ukuran file =108KB
4.	Input citra 3	
	“mynadia.tif”	Dimensi = 256x256x3uint8, Ukuran file =157KB
	“lena.tiff”	Dimensi = 256x256x3uint8, Ukuran file =194KB



Gambar 3. (a) citra asli “mynadia”, (b) cipher citra “mynadia”, (c) citra dekripsi “mynadia”, (d) citra asli “lena” (e) cipher citra “lena” dan (f) citra dekripsi “lena”

Tabel 2. Hasil cipher terhadap format citra

Format Citra	PSNR (dB)		
	R	G	B
lena.jpg	34.56	35.92	33.43
lena.png	52.30	53.81	51.94
lena.tiff	52.30	53.81	51.94

B. *Hasil dan Analisa Cipher Terhadap Format Citra Digital Berbeda.*

Pada Tabel 2, terdapat hasil pengujian *cipher* pada citra digital yang sama tetapi pada format citra digital yang berbeda., yaitu "lena.jpg," "lena.tiff" dan "lena.png". Pada pengujian tersebut dibandingkan citra asli dengan citra dekripsi dengan menggunakan *Peak Signal Noise Ratio* (PSNR).

PSNR digunakan untuk mengukur kualitas citra hasil dekripsi. Semakin besar nilai PSNR, semakin baik kualitas citra digital dekripsi yang dihasilkan. Untuk mengukur PSNR pada citra digital *truecolor* (RGB), dilakukan terpisah pada masing-masing struktur warna. Dengan penerapan *cipher* baru, "jpg" memiliki PSNR > 30dB, sedangan "tiff " dan "png" memiliki PSNR > 50dB. Hal ini menunjukkan bahwa *cipher* sangat baik digunakan untuk proses enkripsi dan dekripsi citra digital dengan format "tiff " dan "png" karena memiliki PSNR yang besar.

C. *Hasil dan analisa cipher pada ukuran citra berbeda terhadap waktu proses .*

Pada Tabel 3, merupakan hasil pengujian *cipher* pada proses enkripsi dan dekripsi untuk ukuran citra asli yang berbeda dibandingkan terhadap waktu proses enkripsi dan dekripsi. Untuk semua ukuran citra asli yang diuji, cipher membutuhkan waktu proses enkripsi dan dekripsi rata-rata 0.06105 detik atau kurang dari 1 detik.

Waktu proses tersebut dipengaruhi juga oleh kemampuan prosessor dari komputer yang digunakan untuk menjalankan Matlab R2010a. Ukuran citra digital yang lebih besar, tidak selalu membutuhkan waktu proses yang lama namun dipengaruhi juga oleh format citra digital. Seperti "mynadia.png" dengan ukuran 63KB, membutuhkan waktu lebih lama dari "mynadia.tiff" dengan ukuran 157KB.

D. *Analisa Histogram Citra Digital*

Pada Gambar 4(a-c) tampak histogram dari citra asli " lena" untuk masing-masing matrik R, G dan B. Sedangkan pada Gambar 4(d-f) tampak histogram dari *cipher* citra "lena" untuk masing-masing matrik R, G dan B.

Histogram merupakan gambaran secara grafis distribusi intensitas *pixel-pixel* di dalam citra tersebut. Frekuensi kemunculan intensitas *pixel-pixel* dapat dimanfaatkan oleh penyerang untuk menganalisa kunci-

Tabel 3. Hasil cipher terhadap waktu proses

Format Citra	Ukuran Citra Asli (KB)	Waktu Proses (dt)
mynadia.jpg	10	0.0574
lena.jpg	20	0.0657
mynadia.png	63	0.0680
lena.png	108	0.0571
mynadia.tiff	157	0.0602
lena.tiff	194	0.0579

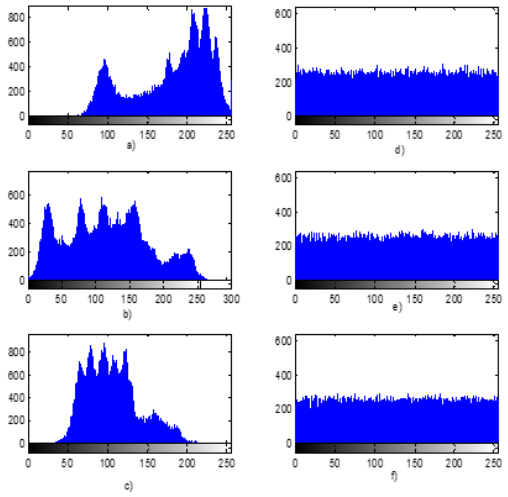
kunci yang mungkin dari citra asli. Supaya penyerang sulit melakukan serangan dengan analisa statistik, maka penting menghasilkan histogram *cipher* citra yang tidak memiliki kemiripan secara statistik dengan histogram citra asli.

Histogram citra asli yang dihasilkan pada Gambar 4(a-c) tidak memiliki kemiripan dengan histogram *cipher* citra pada Gambar 4(d-f). Hal ini disebabkan karena telah terjadi transformasi struktur warna pada *cipher* citra menjadi L*a*b, sedangkan yang ditampilkan pada histogram adalah RGB (*Red, Green, Blue*). Dengan demikian penyerang semakin sulit untuk melakukan penyerangan pada *cipher* citra.

E. *Pengujian dan Analisa Kekuatan Cipher*

Untuk mengukur kekuatan *cipher* baru dan kunci dari serangan *brute-force attack*, maka dapat diukur dari kemungkinan kunci yang harus ditemukan untuk mendekripsi *cipher* terenkripsi. Untuk membuat brute-*force attack* sulit dilakukan, maka jumlah kemungkinan rentang kunci harus dibuat besar sebesar mungkin. Rentang kunci menyatakan jumlah total kunci yang berbeda yang dapat digunakan untuk enkripsi maupun dekripsi.

Pada *cipher* baru ini kunci ditentukan oleh parameter



Gambar 4. (a-c) Histogram citra asli "lena" untuk masing-masing matriks R,G,B .(d-f) Histogram cipher citra "lena untuk masing-masing matrik R, G, B.

L*, a*, b*, λ, X, Y, dan Z. Pada penelitian ini citra digital asli yang digunakan RBG atau *truecolor* yang menggunakan *unsigned integer* (*uint*) 8 dan 16 . Sehingga kemungkinan rentang kunci dari *cipher* baru ini untuk citra digital uint8 adalah:

$$P\left(L^*, a^*, b^*, \lambda, X, Y, Z\right) \approx \left(2^8\right)^7 = 7.25x10^{16}.$$

Sedangkan untuk citra digital uint 16 adalah:

$$P\left(L^*, a^*, b^*, \lambda, X, Y, Z\right) \approx \left(2^{16}\right)^7 = 5.2x10^{33}.$$

Kemungkinan rentang kunci yang dihasilkan cukup besar terhadap serangan *brute-force attack*. Kekuatan kunci dengan *cipher* baru pada citra digital RGB diperoleh untuk unsigned integer 16.

V. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka diperoleh bahwa CIELab dan *chaos* dapat diterapkan sebagai *cipher* pada proses enkripsi dan dekripsi untuk aplikasi kriptografi citra digital dengan waktu proses kurang dari 1 detik. Dengan kemungkinan rentang kunci maksimum pada citra RGB sebesar 5.2x1033 *cipher* cukup aman terhadap serangan *brute-force attack*. Kualitas citra dekripsi diperoleh maksimal dengan PSNR lebih besar dari 50 dB untuk format citra digital "tiff " dan "png".

REFERENSI

[1] W. Gibson, *Neuromancer: 20th Anniversary Edition*, New York, NY: Ace Books, 2004.

[2] Dony Ariyus, *Computer Security*, Yogyakarta, Indonesia: Penerbit ANDI, 2006.

[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] J. Scharinger, "Fast encryption of image data using chaotic Kolmogrov flow," *J. Electronic Eng*. 7, 1998.

[5] J. C. Yen and J. I. Guo, "A new image encryption algorithm and its VLSI architecture," in *Proceedings of the IEEE workshop signal processing systems*, 1999.

[6] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *The Journal of Systems and Software 58*, 2001.

[7] M. A. B. Younes, "Image encryption using block-based transformation algorithm," *IAENG Internatinal Journal of Computer Science*, vol. 35, no. 1, 2008.

[8] N. S. Kulkarni, R. Balasubrmanian, and I. Gupta, "Selective encryption of multimedia images," in *Proceeding off XXXII National Systems Conference*, Dec. 2008.

[9] J. M. Blackledge, M. Ahmad, and O. Faruq, "Chaotic image encryption on frequency domain scrambling," in *Information Processing Letters*, 2010.

[10] H. Khanzadi, "Image encryption based on gyrator transformation using chaotic maps," *ICSP IEEE International Conference*, 2010.

[11] C. K. Nayak, "Image Encryption Using an Enhanced Block based Transformation Algorithm", *International Journal of Research and Review in Computer Science*, vol. 2, no.2, Apr. 2011.

[12] A. M. Somaya, "A new chaos–based image-encryption and compression algorithm", *Journal of Electrical and Computer Enginerring*, 2012.

[13] L. O. Sari, "Perancangan perangkat lunak kriptografi citra digital dengan FFT kunci chaos", *Prosiding SNTIKI 4*, 2012.

[14] G. Hoffmann, *CIE Color Space*, 2010.

[15] G. Sharma, R. C. Eduardo, "The dark side of Cielab," *Proceedings SPIE 8292*, 2012.

[16] P. Ganesan, V. Rajini, and R. I. Rajkumar, "Segmentation and edge detection of color images using CieLab color space and edge detectors," in *International Conference on Emerging Trends in Robotics and Communcation Technologies (INTERACT)*, 2010.

[17] V. Patidar, K. K. Sud, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," Sir Padmapat Singhania University, Bhatewar, India, 2008.

Penerbit:
Jurusan Teknik Elektro, Fakultas Teknik, Universitas Syiah Kuala
Jl. Tgk. Syech Abdurrauf No. 7, Banda Aceh 23111
website: http://jurnal.unsyiah.ac.id/JRE
email: rekayasa.elektrika@unsyiah.net
Telp/Fax: (0651) 7554336