

# ENKRIPSI DAN DEKRIPSI CITRA MENGUNAKAN MODIFIKASI ALGORITMA VIGENERE CIPHER

Risnaty Utami Marsal<sup>#1</sup>, Fitri Arnia<sup>\*2</sup>, Ramzi Adriman<sup>#3</sup>

Jurusan Teknik Elektro dan Komputer, Universitas Syiah Kuala

Jln. Tgk. Syekh Abdurrauf No. 7 Kopelma Darussalam Kecamatan Syiah Kuala, Kota Banda Aceh, Provinsi Aceh, Indonesia

<sup>1</sup>risnatyutamimarsal.inna@gmail.com

<sup>2</sup>fitri.arnia@unsyiah.ac.id

<sup>3</sup>ramzi.adriman@unsyiah.ac.id

**Abstrak**— pengacakan nilai pixel citra merupakan suatu hal yang penting untuk mengamankan informasi yang terkandung dalam citra. Penelitian ini membahas proses enkripsi dan dekripsi pada citra dengan cara mengacak nilai pixel citra menggunakan Algoritma Vigenere Cipher yang kuncinya telah dimodifikasi menggunakan pembangkit bilangan acak Linear Congruent Generator. Dengan menggunakan modifikasi Algoritma Vigenere Cipher citra yang dienkripsi menjadi sangat acak dan mampu menghilangkan informasi visual dari citra asli. Citra yang sudah dienkripsi juga bisa dikembalikan kebentuk semula dengan proses dekripsi. Metode Kasiski yang efektif untuk menentukan panjang kunci pada enkripsi pesan teks ternyata tidak bisa digunakan untuk menentukan panjang kunci yang dihasilkan dengan pembangkit bilangan acak Linier congruent Generator karena kunci yang dibangkitkan berupa angka sehingga tidak ada kriptogram yang berulang.

**Kata Kunci**— Enkripsi, Dekripsi, Vigenere Cipher, Linear Congruent Generator, metode kasiski

## I. PENDAHULUAN

Citra digital menyimpan informasi yang disajikan secara visual, berupa susunan warna yang membentuk sebuah objek. Informasi tersebut diterima oleh indra penglihatan manusia karena informasi yang terdapat di dalam citra tersebut sama dengan yang sesungguhnya. Citra digital adalah fungsi  $f(x,y)$  berukuran M baris dan N kolom, dengan  $x$  dan  $y$  adalah koordinat spasial, dan amplitudo  $f$  di titik koordinat  $(x,y)$  dinamakan intensitas atau tingkat keabuan pada citra di titik tersebut dan nilai  $x,y$  serta nilai amplitudo  $f$  secara keseluruhan berhingga (*finite*) dan bernilai diskrit [1].

Keamanan informasi menjadi sangat penting dalam pertukaran data dan penyimpanan. Ada banyak penggunaan gambar dalam proses medis dan industri, sehingga perlu mempertahankan data gambar rahasia dari akses dan pengungkapan pihak yang tidak sah. Salah satu cara untuk mengamankan informasi yang terdapat pada sebuah citra

adalah melalui pengacakan citra. Pengacakan citra digunakan untuk mengelabui pandangan manusia, sehingga manusia tidak dapat mengartikan objek yang terdapat di dalam citra tanpa bantuan komputer [2].

Dalam hal menyembunyikan pesan citra digital, maka dilakukan enkripsi pada citra sehingga informasi citra rahasia tersebut tidak dapat diakses oleh pihak lain. Pada penelitian sebelumnya, Loukhaoka dkk, mengusulkan algoritma enkripsi dengan mengacak gambar menggunakan prinsip kubus rubik [3]. Sedangkan Kaur [4], melakukan enkripsi digital berdasarkan arsitektur permutasi dan difusi yang dilakukan pada baris dan kolom citra sehingga mengubah dan mengacak posisi piksel.

Salah satu metode enkripsi yang digunakan adalah algoritma *Vigenere Cipher*. Soofi dkk, menggunakan Algoritma *Vigenere Cipher* untuk mengenkripsi teks alfabet dengan menggunakan serangkaian *caesar cipher* yang berbeda berdasarkan huruf kata kunci [5]. Pada penelitian lain, Sembiring [6] melakukan pengacakan citra dengan mengganti warna RGB setiap pixel dan mengubah posisi setiap pixel dari citra yang akan dienkripsi. Sedangkan Suwiryo dkk [7] melakukan pengacakan pada citra bitmap 24-bit menggunakan algoritma vigenere cipher yang digabungkan dengan logistic map untuk membangkitkan bilangan secara acak.

Penelitian ini bertujuan memodifikasi algoritma *Vigenere Cipher* sehingga dapat digunakan untuk enkripsi citra digital yang kemudian disebut Algoritma Transformasi *Vigenere Cipher*. Modifikasi dilakukan pada nilai modulus yang akan digunakan. Pada algoritma *Vigenere Cipher* klasik, nilai modulusnya adalah 26 karena dalam huruf alfabet hanya ada 26 karakter, sedangkan pada citra digital nilai intensitas sebuah piksel ada 256 sehingga nilai modulus diubah menjadi 256. Modifikasi juga dilakukan pada proses pembangkitan kunci. Pembangkit kunci pada algoritma *Vigenere Cipher* klasik menggunakan sederetan kata. Algoritma tersebut dapat dipecahkan dengan menggunakan

metode Kasiski. Pada Algoritma Transformasi *Vinegere Cipher* kunci dimodifikasi menggunakan *linear congruent generator*, sehingga akan didapatkan kunci berupa deretan bilangan acak. Algoritma Transformasi *Vinegere Cipher* akan diuji menggunakan Metode Kasiski yang sebelumnya mampu memecahkan algoritma *Vinegere Cipher* klasik.

Selanjutnya, artikel ini diorganisasikan sebagai berikut: pada bagian 2 dibahas metode dan perancangan sistem. Pada bagian 3 akan dibahas tentang hasil dan analisis, sedangkan pada bagian 4 akan dirangkum sejumlah kesimpulan dari penelitian ini.

II. METODE

Penelitian ini menggunakan citra yang disiapkan yaitu berukuran 960 x 960 seperti pada Gambar 1. Citra yang disiapkan berupa citra foto *truecolor*, citra foto *grayscale*, citra biner dengan format penyimpanan *jpg*, *bmp* dan *png*, citra *magnetic resonance* yang digunakan dalam dunia medis, citra pankromatik yang digunakan dalam penginderaan jauh dan citra sidik jari dalam dunia forensik (Gambar 2).



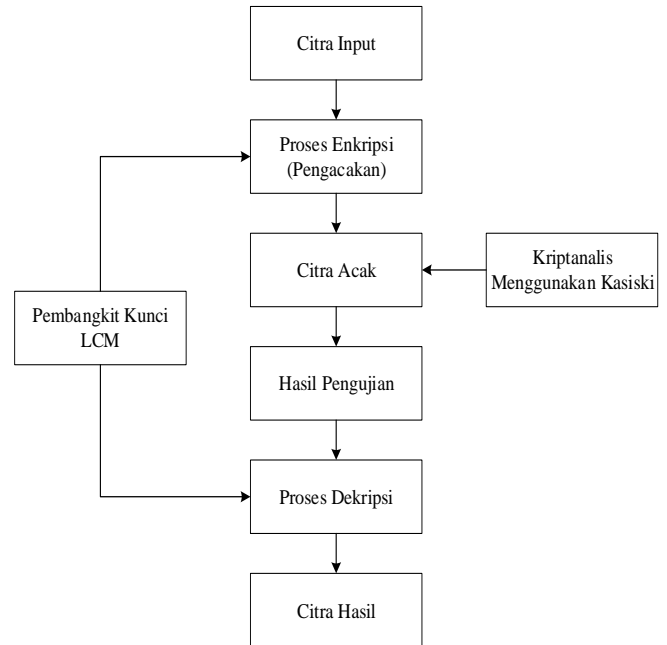
Gambar 1. Citra hasil cropping 8x8 pixel dari ukuran asli 960 x 960 pixel

Gambar 2 memperlihatkan tahapan penelitian. Citra input yang digunakan. Pada proses memodifikasi *Vinegere Cipher* klasik [6, 8], maka nilai modulus yang sebelumnya digunakan untuk enkripsi dan dekripsi pesan teks adalah bernilai 26 (jumlah huruf alfabet) diubah menjadi jumlah nilai intensitas sebuah piksel pada citra yaitu 256. Persamaan (1) digunakan untuk proses enkripsi  $C_i$ , sedangkan persamaan (2) digunakan untuk proses dekripsi  $P_i$ .

$$C_i = (P_i + ((aZ_{i-1} + c) \bmod 256)) \bmod 256 \tag{1}$$

$$P_i = (P_i - ((aZ_{i-1} + c) \bmod 256)) \bmod 256 \tag{2}$$

Proses enkripsi citra digital rentang nilai piksel adalah antara 0 sampai 255 maka dalam hal ini dengan menggunakan modulus 256 maka akan terjadi perulangan kembali nilai piksel ke 0 jika nilai piksel tersebut telah mencapai 256. Proses enkripsi dilakukan pada citra foto *truecolor*, citra foto *grayscale*, citra biner dengan format penyimpanan *jpg*, *bmp* dan *png*, citra *magnetic resonance* dan citra pankromatik.



Gambar 2. Diagram proses enkripsi dan dekripsi algoritma Transformasi *Vinegere Cipher* dengan uji kriptanalisis menggunakan metode Kasiski.

Pada proses membangkitkan kunci pada *Vinegere Cipher* klasik digunakan *Linear Congruent Generator* yang membangkitkan bilangan acak dengan distribusi uniform [7, 9]. Modulus  $m$  yang digunakan untuk membangkitkan kunci dengan *Linear Congruent Generator* pada penelitian ini juga diubah menjadi 256 dengan faktor pengali  $a$ ,  $Z_{i-1}$  merupakan bilangan acak sebelumnya dan penambahan increment  $c$  untuk perulangan pengacakan.

$$Z_i = (aZ_{i-1} + c) \bmod m \tag{3}$$

*Linear Congruent Generator* mempunyai periode penuh  $(m-1)$  jika memenuhi syarat sebagai berikut :

- a.  $c$  relatif prima terhadap  $m$
- b.  $a-1$  dapat dibagi dengan semua faktor prima dari  $m$
- c.  $a-1$  adalah kelipatan 4 jika  $m$  adalah kelipatan 4
- d.  $m > \max(a, c, Z_0)$
- e.  $a > 0, c > 0$

Keacakan kunci yang dihasilkan sangat tergantung dari variabel yang dijadikan sebagai nilai *input* dimana setiap variabel harus memenuhi syarat pengulangan penuh. Setelah membangkitkan kunci langkah selanjutnya adalah melakukan proses enkripsi.

Untuk mengetahui hasil enkripsi citra maka diperlukan metode pengujian. Pengujian akan dilakukan terhadap citra hasil enkripsi dan kunci yang telah dibangkitkan. Proses pengujian terhadap citra hasil enkripsi menggunakan uji entropy.

Uji Entropy digunakan untuk mengetahui keragaman dari intensitas citra. Nilai entropy besar untuk citra dengan transisi derajat keabuan merata dan bernilai kecil jika struktur citra tidak teratur. Sehingga semakin tinggi nilai entropy maka cipherimage yang dihasilkan semakin baik, sebaliknya jika nilai entropy semakin rendah maka

cipherimage yang dihasilkan memiliki kualitas yang semakin rendah. Nilai *entropy* dihitung menggunakan Persamaan berikut[10] :

$$H_e = -\sum_{k=0}^{255} P(k) \cdot \log_2(P(k)) \text{ (bit/symbol)} \quad (4)$$

Di mana :

$H_e$  : Nilai *entropy*

G : Derajat keabu-abuan citra masukkan (dari 0-255)

P(k) : Probabilitas symbol ke-k

Uji *entropy* juga akan digunakan untuk mengukur kekuatan variasi kunci yang digunakan pada citra lena. Selain itu metode kasiski juga akan digunakan untuk mengukur seberapa akurat metode ini dalam menebak panjang kunci yang digunakan untuk proses enkripsi citra tersebut.


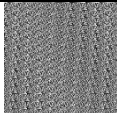

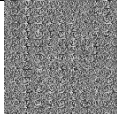
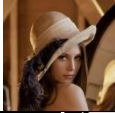


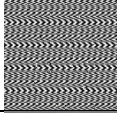



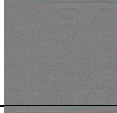








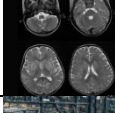




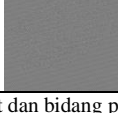
Metode Kasiski memanfaatkan kelemahan *Vigenere Cipher* yang menggunakan kunci yang sama berulang-ulang sehingga menghasilkan potongan cipherteks yang sama untuk plainteks yang sama. Cara kerja metode Kasiski ini memiliki beberapa langkah berikut ini [9, 10] :

1. Temukan semua kriptogram yang berulang di dalam *ciphertext* (pesan yang panjang biasanya mengandung kriptogram yang berulang)
2. Hitung jarak antara kriptogram yang berulang
3. Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin)
4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut. Nilai tersebut kemungkinan adalah panjang kunci yang digunakan oleh algoritma *vigenere cipher*.

Setelah melalui serangkaian proses mengacak citra dan pengujian enkripsi dengan metode Kasiski maka langkah selanjutnya adalah proses pengembalian nilai piksel citra yang telah teracak ke nilai semula dalam hal ini disebut dengan proses dekripsi. Kunci yang digunakan pada proses dekripsi harus sama dengan kunci yang digunakan pada proses enkripsi, jika kunci yang digunakan tidak sama maka nilai piksel dari citra tersebut tidak akan kembali ke nilai semula.

### III. HASIL DAN PEMBAHASAN

Dari penelitian yang telah dilakukan, algoritma Transformasi *Vigenere Cipher* dengan pembangkit kunci bilangan acak *linear congruent generator* dapat mengacak nilai piksel citra digital, sehingga hasil analisa tersebut dapat diterapkan ke berbagai jenis citra.

no	Nama dan format file	Citra (plainimage)	Resolusi dan bit	Citra (cipherimage)
1	Lena1.jpg		960x960 (8 bit)	
2	Lena2.jpg		960x960 (8 bit)	
3	Lena3.jpg		960x960 (24 bit)	
4	Biner1.jpg		960x960 (8 bit)	
5	Truecolor.jpg		960x960 (24 bit)	
6	Traveling.jpg		960x960 (24 bit)	
7	Traveling.bmp		960x960 (24 bit)	
8	Lena.bmp		960x960 (24 bit)	
9	Traveling.png		960x960 (24 bit)	
10	Lena.png		960x960 (24 bit)	
11	Mri.jpg		960x960 (24 bit)	
12	Pankromatik.jpg		960x960 (24 bit)	
13	forensik.jpg		960x960 (8 bit)	

Tabel 1. citra berdasarkan kedalaman warna, format dan bidang penerapan menggunakan kunci  $z=3$ ,  $a=5$  dan  $c=17$

Pengujian pertama adalah mencari nilai *entropy* pada cipherimage untuk setiap resolusi. Nilai *entropy* digunakan untuk mengetahui keragaman intensitas dari sebuah citra.




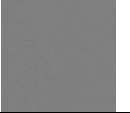






Semakin tinggi nilai entropy maka menunjukkan suatu citra memiliki intensitas citra yang beragam dan transisi derajat keabuan yang merata.

No	Citra uji	Plainimage	Cipherimage	Selisih
1	Lena1.jpg	1,459661	7,999994	6,540333
2	Lena2.jpg	1,484369	7,999964	6,515594
3	Lena3.jpg	1,568000	7,999985	6,431984
4	Biner1.jpg	1,879288	7,999455	6,120167
5	Truecolour.jpg	1,683474	7,999900	6,316426
6	Traveling.jpg	7,319908	7,999915	0,680006
7	Traveling.bmp	7,411882	7,999633	0,587750
8	Lena.bmp	7,568000	7,999985	0,431984
9	Traveling.png	7,516512	7,999860	0,483348
10	Lena.png	7,568000	7,999985	0,431984
11	Mri.jpg	6,100380	7,999664	1,899283
12	Pankromatik.jpg	7,412677	7,999934	0,587256
13	Forensik.jpg	2,672569	7,999976	4,740119

Tabel 2. Uji Entropy pada plainteks dan cipberteks

Berdasarkan tabel 2 dapat dilihat semua cipherimage mengalami perubahan nilai entropy dari citra awal dengan selisih terkecil sebesar 0,431984 dan selisih terbesar 6,540333. Semakin tinggi nilai entropy maka cipherimage yang dihasilkan semakin baik, dan sebaliknya jika nilai entropy semakin rendah maka cipherimage yang dihasilkan memiliki kualitas yang semakin rendah.

Pengujian kedua dilakukan pada citra lena dengan mencoba beberapa variasi variabel kunci a dan c yang harus memenuhi syarat linier congruent method dengan penambahan nilai terdekat. Sedangkan untuk nilai z tetap bernilai 17 dan modulus 256. Setelah itu dilakukan uji entropy pada cipherimage untuk melihat pada variable mana terjadi perubahan nilai entropy terkecil dan terbesar.

No	a	c	Plainimage	Cipherimage
1	5	3		
2	9	5		
	13	7		
4	17	9		
5	21	11		

Tabel 3. Hasil enkripsi citra dengan variasi variabel kunci









Berikut ini akan disajikan hasil uji entropy terhadap cipherimage yang menggunakan variasi variabel kunci.

Kunci ke	Plainimage	Cipherimage	Selisih
1	7,568000	7,999982	0,431982
2	7,568000	7,999986	0,431986
3	7,568000	7,999984	0,431984
4	7,568000	7,999983	0,431983
5	7,568000	7,999983	0,431983

Tabel 4. Uji Entropy dengan variasi kunci

Berdasarkan tabel 3 dapat dilihat semua cipherimage mengalami penambahan nilai entropy. Walaupun nilai a dan c memakai penambahan nilai terdekat, namun trend penambahan nilai entropy tidak bisa diprediksi. dari kunci pertama ke kunci ke 2 terjadi penambahan nilai selisih tapi kemudian nilai selisih kembali turun pada kunci ke 3, dan cenderung tetap pada kunci ke 4 dan ke 5. Dari hasil uji entropy pada tabel 2 dan 3 dapat dikatakan kunci yang digunakan cukup kuat untuk melakukan enkripsi citra karena terjadi penambahan nilai entropy dari citra awal sehingga cipherimage yang dihasilkan memiliki intensitas citra yang beragam dan transisi derajat keabuan yang merata dibandingkan dengan citra awal.

Sebagai perbandingan, penelitian Suwiryo dkk [7] dengan judul enkripsi citra digital menggunakan vigenere cipher dan logistic map juga memakai Uji entropy untuk menguji cipherimage yang dihasilkan. Citra yang digunakan adalah citra bitmap-24 bit. Berikut hasilnya

No	Nama File	Citra (plainimage)	Resolusi	Citra (cipherimage)
1	car.bmp		1024x768	
2	harimau.bmp		640x480	
3	salena.bmp		227x329	
4	rumah.bmp		125x122	

Gambar 3. tabel Plainimage dan cipher image penelitian sebelumnya

Citra Uji		Citra Awal	Percobaan		
			I	II	III
Entropy	car.bmp	7,636	7,994	7,994	7,991
	harimau.bmp	7,299	7,992	7,990	7,986
	salena.bmp	6,412	7,949	7,965	7,958
	rumah.bmp	7,232	7,962	7,974	7,972

Gambar 4. Tabel hasil uji entropy penelitian sebelumnya

Pengujian ketiga dilakukan untuk menguji panjang kunci yang dibangkitkan dengan Linier congruent Method menggunakan Metode kasiski dimana sebelumnya telah terbukti bisa menebak panjang kunci pada enkripsi teks. Metode kasiski memanfaatkan keuntungan bahwa bahasa inggris tidak hanya mengandung perulangan huruf tetapi juga perulangan pasangan huruf atau tripel huruf. Perulangan kelompok huruf ini ada kemungkinan untuk menghasilkan kriptogram yang berulang

Namun hal seperti yang telah dijelaskan di atas tidak akan terjadi jika kunci yang digunakan adalah kunci acak atau kunci yang disusun dari deretan angka sehingga tidak akan di temukan perulangan poligram dari sebuah kata. Oleh karena itu metode kasiski tidak dapat digunakan untuk menghitung panjang kunci yang digunakan.. Untuk simulasi digunakan 64 kunci dimana untuk melihat perulangan kunci maka kunci yang digunakan sebelumnya di konversi menggunakan kode ASCII

#### IV. KESIMPULAN

Berdasarkan penelitian yang telah di lakukan maka dapat diambil kesimpulan sebagai berikut :

1. Modifikasi algoritma *vigenere cipher* menggunakan pembangkit bilangan acak *linear congruent generator* dapat digunakan untuk mengacak nilai piksel citra digital.
2. Modifikasi algoritma *vigenere cipher* menggunakan pembangkit kunci bilangan acak *linear congruent generator* dapat diterapkan untuk mengacak citra dengan berbagai format penyimpanan, seperti jpg, bmp, dan png

- juga dapat diterapkan untuk mengacak citra dengan berbagai bidang penerapannya, misalnya di bidang biomedis, bidang penginderaan jauh dan bidang forensik.
3. Hasil pengujian nilai entropy menunjukkan semua cipherimage mengalami penambahan nilai entropy sehingga bisa disimpulkan algoritma *vigenere cipher* dengan modifikasi kunci menggunakan linear congruent method cukup kuat untuk mengenkripsi citra
  4. Algoritma kasiski tidak dapat diterapkan untuk mencari panjang kunci yang digunakan pada modifikasi *vigenere cipher* karena kunci yang dibangkitkan tidak mengandung deretan kata.

#### REFERENSI

- [1] R. Sadikin, Kriptografi Untuk Keamanan Jaringan, Yogyakarta: Andi Offset, 2012.
- [2] I. Saputra, M. N. A. Hasibuan dan R. Rahim, "Vigenere Cipher With Grayscale Image Generator for Secure Text File," International Journal of Engineering & Technology (IJERT), vol. VI, no. 1, pp. 266-269, 2016.
- [3] K. Loukhaoukha, J.Chouinard, dan A. Berdai "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, Volume 2012, Article ID 173931
- [4] A. A. Soofi, I. Riaz dan U. Rasheed, "An Enhanced Vigenere Cipher For Data Security," International Journal of Scientific & Technology Researcher, vol. III, no. 5, pp. 141-145, 2016.
- [5] N. Kaur dan R. Mahajan, "An Improved Scheme of Embedded Extended Visual Cryptography," International Journal of Computer Engineering & Science (IJCES), vol. IV, no. 2, pp. 69-73, 2014.
- [6] M. E. S dan A. P, "Linear Congruential Generator for LUT-SR Architecture," International Journal of Scientific Engineering and Research (IJSER), vol. II, no. 3, pp. 97-102, 2014
- [7] R. Munir, Kriptografi, Bandung: Informatika, 2006.
- [8] C. J. Kung dan H. C. Tang, "Criterion of Spectral Test for Linear Congruential Random Number Generators," Tamkang Journal of Science and Engineering, vol. III, no. 12, pp. 365-369, 2009
- [9] D. Putra, Pengolahan Citra Digital, Yogyakarta: Andi Offset, 2010.
- [10] Y. Kurniawan, Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika, 2004