Volume 18 Nomor 2, September 2018 ISSN 1411-6669

MIMS

MAJALAH ILMIAH

Matematika dan Statistika

DITERBITKAN OLEH:
JURUSAN MATEMATIKA
FMIPA - UNIVERSITAS JEMBER

MAJALAH ILMIAH
Matematika dan Statistika

Alamat Redaksi:
Jurusan Matematika FMIPA – Universitas Jember
Jalan Kalimantan No 37 Kampus Tegalboto Jember 68121
Telp. : (0331) 334293
E-mail: mims.fmipa@unej.ac.id
Website: https://jurnal.unej.ac.id/index.php/MIMS/index

Diterbitkan oleh : Jurusan Matematika – FMIPA Universitas Jember.
Tahun pertama terbit : Oktober 2000
Jumlah terbit : Dua kali setahun pada bulan Maret dan September
Gambar cover depan : rancang bangun geometri, iterasi dan regresi

Majalah Ilmiah Matematika dan Statistika	Volume 18 Nomor 2	Halaman: 55 – 104	Jember, September 2018	ISSN 1411-6669

MAJALAH ILMIAH
Matematika dan Statistika

Volume 18 Nomor 2, September 2019 **ISSN 1411-6669**

Daftar Isi

Majalah Ilmiah Matematika dan Statistika Volume 18 Nomor 2, 2018, 91 – 104
https://jurnal.unej.ac.id/index.php/MIMS/index ISSN 1411-6669

PENGAMANAN *IMAGE* DENGAN MODIFIKASI ALGORITMA *ELECTRONIC CODE BOOK* (ECB)

(*Image Security Using Modified Electronic Code Book (ECB) Algorithm*)

Melinda Asti, Ahmad Kamsyakawuni, Kiswara Agung Santoso

Jurusan Matematika, Fakultas MIPA, Universitas Jember
Jl. Kalimantan 37 Jember 68121, Indonesia
E-mail: mela.asti@gmail.com, {kamsyakawuni, kiswara}.fmipa@unej.ac.id

Abstract. Cryptography is knowledge of encoding data to ensure the confidentiality, security, validity and integrity of data. Cryptography is divided into two namely classical cryptography and modern cryptography. One example of modern cryptography is the Electronic Code Book (ECB). Electronic Code Book (ECB) is a modern cryptographic method used to encrypt and decrypt text, images and more. The image is formed from several pixels which consist of several bits in a pixel. Bits are divided into two namely Least Significant Bit (LSB) and Most Significant Bit (MSB).LSB is the four rightmost bits while MSB is the leftmost four bits of a pixel. The purpose of this study is to compare the level of security of Electronic Code Book (ECB) image security results with the results of securing an Electronic Code Book (ECB) modified image. The data used in this study are 8 RGB and Greyscale images also a key in the form of one ASCII character. The results obtained show that securing images with modified Electronic Code Book (ECB) is safer than securing images with Electronic Code Book (ECB) based on histogram analysis, differential analysis and correlation coefficients.

Keywords: ASCII, Electronic Code Book (ECB), Most Significant Bit (MSB)
MSC2010: 94A60

1. Pendahuluan

Perkembangan teknologi dan informasi saat ini semakin canggih, salah satunya yaitu pada pengiriman pesan. Pengiriman pesan biasanya rentan terhadap pengaksesan oleh pihak ketiga. Hal ini menyebabkan isi pesan yang dikirim dapat diketahui oleh pihak ketiga. Solusi untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah teknik enkripsi dan dekripsi Ilmu yang mempelajari tentang teknik enkripsi dan deskripsi pesan, data, maupun informasi disebut Kriptografi.Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi. Kriptografi dibagi menjadi 2 yaitu kriptografi klasik dan kriptografi modern. Salah satu contoh kriptografi modern yaitu *Electronic Code Book* (ECB). *Electronic Code Book* (ECB) merupakan metode kriptografi modern yang digunakan untuk mengenkripsi dan mendekripsi teks, citra dan lainnya. Citra terbentuk dari beberapa pixel yang di dalam pixelnya terdiri dari beberapa bit. Bit dibagi menjadi 2 yaitu *Least Significant Bit* (LSB) dan *Most Significant Bit* (MSB). LSB merupakan 4

bit yang letaknya paling kanan sedangkan MSB merupakan 4 bit yang letaknya paling kiri dari sebuah pixel.

Beberapa penelitian sebelumnya yaitu Mufid melakukan penelitian Teknik Enkripsi dan Deskripsi menggunakan Algoritma *Electronic Code Book* (ECB) menghasilkan *plainteks* yang sama jika dienkripsi akan menghasilkan *cipher teks* yang sama. Hutabalian melakukan penelitian Perancangan Perangkat Lunak Pengamanan File Menggunakan Algoritma *Electronic Code Book* (ECB) menghasilkan *plainteks* yang sama jika deskripsi akan menghasilkan *cipher teks* yang sama juga. Wahyuni melakukan penelitian Implementasi Steganografi dalam menyembunyikan Pesan Teks dengan Metode MSB (*Most Significan Bit)* menghasilkan pesan dapat disembunyikan ke dalam gambar, namun hasil gambar yang telah disisipkan pesan akan berbeda dengan gambar sebelumnya.

2. Metodologi

Data yang digunakan dalam penelitian ini adalah citra RGB dan citra grayscale yang digunakan sebagai *plainimage*. Data yang digunakan untuk pengujian pada penelitian ini sebanyak 8 citra. Gambar 1 – 8 adalah data-data yang digunakan pada penelitian.

Gambar 1. Citra 1

Gambar 2. Citra 2

Gambar 3. Citra 3

Gambar 4. Citra 4


Gambar 5. Citra5


Gambar 6. Citra 6


Gambar 7. Citra 7


Gambar 8. Citra 8

***Electronic Code Book* (ECB)**

Penulis melakukan penelitian dengan perhitungan secara manual. Penulis juga melakukan penelitian menggunakan software MATLAB.Untuk setiap blok *plainimage Pi*, dienkripsi secara individual dan independen menjadi blok *cipherimageCi*. Secara matematis, dinyatakan seperti pada Persamaan (1)

$$Ci = Ek\ (\ Pi\ ) \tag{1}$$

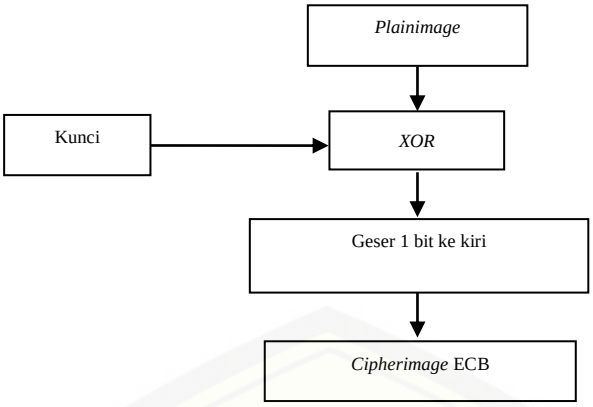
sedangkan dekripsi seperti Persamaan (2)

$$Pi = Dk\ (Ci\ ) \tag{2}$$

Dalam hal ini, *K* adalah kunci dan *Pi* dan *Ci* masing-masing blok *plainimage* dan *cipherimage* ke-*i* [4].

Langkah-langkah enkripsi gambar menggunakan *Electronic Code Book* (ECB) adalah sebagai berikut (lihat pada Gambar 9):

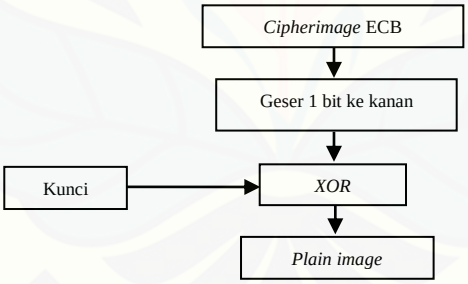
1. Menyiapkan *plain image* dan kunci berupa satu karakter yang dikonversi ke dalam bentuk biner. Bagi *plainimage* dalam bentuk biner menjadi blok-blok yang berukuran 4 bit.
2. Kunci diulang sebanyak bit pada *plain image* kemudian dilakukan operasi XOR dengan *plain image*.
3. Hasil dari operasi XOR digeser tiap blok bit sebanyak satu bit ke kiri dengan blok bit berisi masing-masing 4 bit. Outputnya yaitu *cipherimage ECB*.



Gambar 9. Proses enkripsi *Electronic Code Book* (ECB)

Langkah-langkah dekripsi gambar menggunakan *Electronic Code Book* (ECB) adalah sebagai berikut(lihat Gambar 9):

1. Menyiapkan *Cipherimage ECB* dan kunci berupa teks yang dikonversi ke dalam bentuk biner. Bagi *cipherimage* dalam bentuk biner menjadi blok-blok yang berukuran 4 bit
2. Melakukan pergeseran tiap blok bit sebanyak satu bit ke kanan dengan blok bit berisi masing-masing 4 bit pada *cipherimage ECB.*
3. Kunci diulang sebanyak bit pada *cipherimage ECB* kemudian dilakukan operasi XOR dengan *cipherimage ECB* hasil pergeseran. Output dari tahap ini adalah hasil akhir dari pendekripsian yaitu *plainimage.*



Gambar 10. Proses dekripsi *Electronic Code Book* (ECB)

Modifikasi *Electronic Code Book* (ECB)

Penulis melakukan penelitian dengan mencoba perhitungan secara manual. Data yang dienkripsi berupa *plain image*. Penulis juga melakukan penelitian menggunakan software MATLAB.Langkah-langkah enkripsi gambar menggunakan *Electronic Code Book* (ECB) adalah sebagai berikut (lihat Gambar 11) :

1. Menyiapkan *plainimage* dan kunci berupa satu karakter. *Plainimage* dan kunci dikonversi ke dalam bentuk biner. Bagi *plainimage* dalam bentuk biner menjadi blok-blok yang berukuran 4 bit.
2. Kunci diulang sebanyak bit pada *plain image* kemudian dilakukan operasi XOR dengan *plain image*.

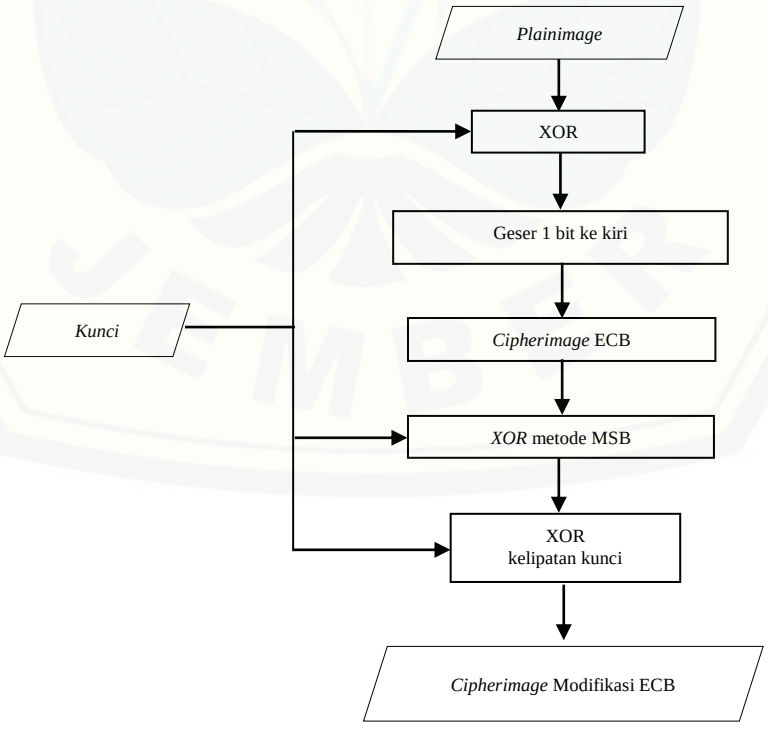
3. Hasil dari operasi XOR digeser tiap blok bit sebanyak satu bit ke kiri dengan blok bit berisi masing-masing 4 bit. Output dari pengenkripsian ini yaitu *cipherimage ECB.*
4. Kemudiankunci dalam bentuk biner sebanyak 8 bit dibagi menjadi 4 blok bit dengan masing-masing berisi 2 bit.

   Contoh: M = 77 = 01001101 = 01 00 11 01

   Setelah itu masing-masing blok bit kunci yang berisi 2 bit, disisipkan 6 bit dibelakangnya dengan "000000" sehingga berjumlah 8 bit dan hasilnya merupakan kunci MSB[2].

   01000000 **00**000000 **11**000000 **01**000000

   Cipherimage ECB di XOR kan dengan perulangan kunci MSB tersebut menggunakan metode MSB menghasilkan *cipherimage.*
5. Hasil dari operasi XOR *Cipher Image ECB* dengan kunci MSB di XOR-kan dengan kelipatan kunci. Misalkan kunci M dikonversi ke desimal menjadi 77. Kelipatan dari 77 yaitu 77, 154, 231, 308, 385, dan seterusnya. Pada citra, pixel yang terdiri dari 8 bit memiliki nilai pixel antara 0 sampai 255 berjumlah 256. Sehingga pada citra digunakan operasi modulo 256 untuk mencari kelipatan kunci dengan perhitungan sebagai berikut : 77 mod 256 = 77, 154 mod 256 = 256, 231 mod 256 = 231, 308 mod 256 = 52, 385 mod 256 = 129. *Cipherimage* MSB di XOR kan dengan perulangan kelipatan kunci modulo 256 sebanyak bit pada *image* MSB menghasilkan *cipherimage modifikasi ECB.*
6. Output dari tahap ini adalah hasil akhir dari pengenkripsian yaitu *cipherimage modifikasi ECB*



Gambar 11. Proses enkripsi modifikasi *Electronic Code Book* (ECB)

Langkah-langkah dekripsi gambar menggunakan *Electronic Code Book* (ECB) adalah sebagai berikut (lihat Gambar 12):

1. Menyiapkan *Cipherimage* dan kunci berupa satu karakter. *Cipherimage* dan kunci dikonversi ke biner.
2. Misalkan kunci M dikonversi ke desimal menjadi 77. Kelipatan dari 77 yaitu 77, 154, 231, 308, 385, dan seterusnya. Pada citra, pixel yang terdiri dari 8 bit memiliki nilai pixel antara 0 sampai 255 berjumlah 256. Sehingga pada citra digunakan operasi modulo 256 untuk mencari kelipatan kunci dengan perhitungan sebagai berikut : 77 mod 256 = 77, 154 mod 256 = 256, 231 mod 256 = 231, 308 mod 256 = 52, 385 mod 256 = 129. *Cipherimage* di XOR kan dengan perulangan kelipatan kunci modulo 256 sebanyak bit pada *cipherimage* menghasilkan *cipherimage MSB.*
3. Kemudian kunci dalam bentuk biner sebanyak 8 bit dibagi menjadi 4 blok bit dengan masing-masing berisi 2 bit.

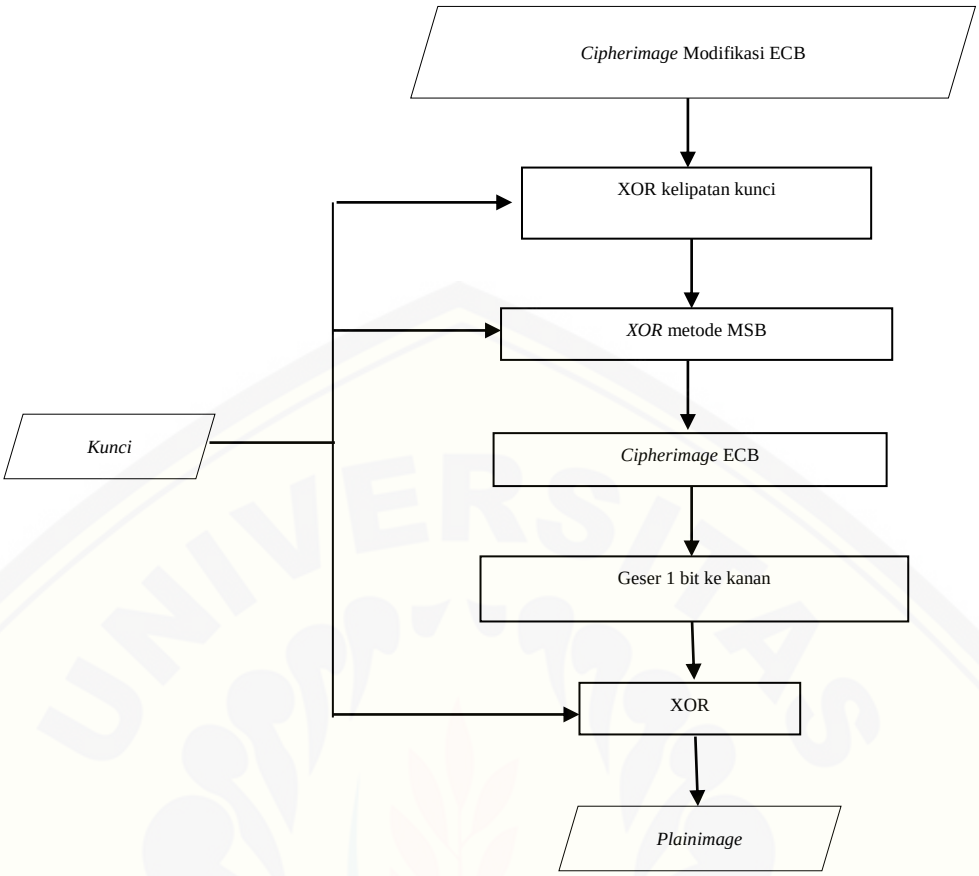
   Contoh: M = 77 = 01001101 = 01 00 11 01

   Setelah itu masing-masing blok bit kunci yang berisi 2 bit, disisipkan 6 bit dibelakangnya dengan “000000” sehingga berjumlah 8 bit dan hasilnya merupakan kunci MSB [2].

   01000000 **00**000000 **11**000000 **01**000000
4. *Cipherimage* MSB di XOR kan dengan perulangan kunci MSB tersebut menggunakan metode MSB menghasilkan *cipherimage ECB.*Bagi *cipherimage ECB* dalam bentuk biner menjadi blok-blok yang berukuran 4 bit. Melakukan pergeseran tiap blok bit sebanyak satu bit ke kanan dengan masing-masing 4 bit pada *cipher image ECB.*
5. Kunci utama diulang sebanyak bit pada *cipher image ECB* kemudian diXOR-kan dengan *cipher image ECB* hasil pergeseran.
6. Output dari tahap ini adalah hasil akhir dari pendekripsian yaitu *plain image.*

Analisis Hasil

Analisis hasil dilakukan setelah mengenkripsi data menggunakan *Electronic Code Book* (ECB) dan menggunakan modifikasi *Electronic Code Book* (ECB) kemudian dihitung hasil histogram, diferensial, dan koefisien korelasi. Dilanjutkan dengan membandingkan hasil perhitungan dari histogram, NPCR, UACI, dan koefisien korelasi. Sehingga dapat dianalisis pengaruh modifikasi pada *Electronic Code Book* (ECB) terhadap peningkatan keamanan *cipher image* yang dihasilkan. Analisis histogram dapat mencerminkan informasi dari penyebaran nilai pixel pada suatu citra. Untuk menganalisis keseragaman histogram dari gambar yang terenkripsi, maka dapat menggunakan pengujian X^2, dimana semakin kecil hasil dari X^2 maka tingkat keseragaman dalam histogram semakin merata dan hasil dari pengenkripsian semakin aman, sedangkan semakin besar hasil dari X^2 maka tingkat keseragaman dalam histogram semakin tidak merata dan hasil dari pengenkripsian semakin tidak aman. Nilai dari X^2 untuk gambar yang terenkripsi dari dimensi $m \times n$ diberikan formula seperti pada Persamaan (3).



Gambar 12. Proses dekripsi modifikasi *Electronic Code Book* (ECB)

$$X^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0} \tag{3}$$

dimana v_i adalah frekuensi yang diamati dari nilai keabuan i $(0 \leq i \leq 255)$ dan v_0 adalah frekuensi yang diharapkan dari sebuah nilai keabuan i, jadi $v_0 = \frac{m \times n}{256}$[3].

Analisis diferensial digunakan untuk mengetahui perbedaan *plainimage* dengan *cipherimage*. Analisis diferensial dapat ditentukan dengan dua indikator pengukuran yang biasa digunakan, yaitu *Number of Pixels Change Rate* (NPCR) dan *Unifer Average Changing Intensity* (UACI). NPCR digunakan untuk mengetahui berapa banyak *pixel* yang berbeda dari dua buah citra, sedangkan UACI berfokus pada interval perbedaan nilai *pixel* dari kedua citra. Perhitungan NPCR didefinisikan seperti pada Persamaan (4).

$$NPCR = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^{o-1} \frac{d_{i,j,k}}{T} \right) \times 100\% \tag{4}$$

dimana T merupakan jumlah total *pixel* di *cipher image*. Untuk menghitung T maka diperlukan m, n, dan o yang melambangkan lebar, tinggi, dan kedalaman citra. Sedangakan $d_{i,j,k}$ melambangkan derajat keabuan dan ditentukan sebagai berikut:

$$d_{i,j,k} = \begin{cases} 0, jika\ c_{i,j,k}^{(1)} = c_{i,j,k}^{(2)} \\ 1, jika\ c_{i,j,k}^{(1)} \neq c_{i,j,k}^{(2)} \end{cases}$$

dimana $c_{i,j,k}^{(1)}$ dan $c_{i,j,k}^{(2)}$ melambangkan nilai keabuan dari baris i, kolom j, dan kanal k dari citra $c^{(1)}$ (*plainimage*) dan $c^{(2)}$ (*cipherimage*).

Sedangkan perhitungan UACI didefinisikan seperti pada Persamaan (5).

$$UACI = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{k=0}^{o-1} \frac{\left| c_{i,j,k}^{(1)} - c_{i,j,k}^{(2)} \right|}{F \times T} \right) \times 100\% \quad (5)$$

dimana F menunjukkan nilai *pixel* terbesar yang kompatibel dengan format cipher image. Batas minimal indikator NPCR untuk mengetahui berapa banyak pixel yang berbeda antara *plainimage* dengan *cipherimage* yaitu sebesar 99,609375% dan batas minimal UACI pada interval perbedaan nilai pixel antara *plainimage* dan *cipherimage* yaitu sebesar 33,463541% untuk citra *grayscale* dan RGB, maka *cipherimage* dikatakan baik apabila memenuhi batas minimal dari indikator NPCR dan UACI. Secara visual, *cipherimage* dikatakan baik apabila sangat "berbeda" dengan citra aslinya dan terlihat acak [1].

Analisis statistik seperti faktor koefisien korelasi digunakan untuk mengukur hubungan antara dua variabel, yaitu *plainimage* dan *cipherimage*. Faktor ini menunjukkan sejauh mana algoritma enkripsi yang diusulkan sangat aman dalam serangan statistik. Oleh karena itu, *cipherimage* harus sepenuhnya berbeda dari *plainimage*. Koefisien korelasi diukur dengan menggunakan Persamaan (6).

$$CorrCoef(x, y) = \frac{\sum_{i=1}^{n} (x_i - \mu(x))(y_i - \mu(y))}{\sigma(x)\sigma(y)} \quad (6)$$

di mana $\mu(x)$ dan $\mu(y)$ adalah rata-rata dari masing-masing x dan y diperoleh dari Persamaan (7).

$$\mu(x) = \frac{1}{n} \sum_{i=1}^{n} x_i \text{ dan } \qquad \mu(y) = \frac{1}{n} \sum_{i=1}^{n} y_i \quad (7)$$

x dan y adalah variabel dari *plainimage* dan *cipherimage*. Standar deviasi (σ) digunakan untuk mengetahui seberapa dekat sebaran data dengan nilai rata-ratanya. Berikut adalah Persamaan (8) tentang standar deviasi untuk masing-masing x dan y.

$$\sigma(x) = \sqrt{\sum_{i=1}^{n}(x_i - \mu(x))^2} \text{ dan } \sigma(y) = \sqrt{\sum_{i=1}^{n}(y_i - \mu(y))^2} \quad (8)$$

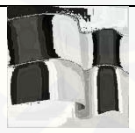
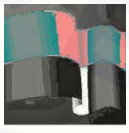
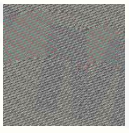
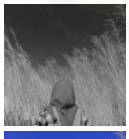
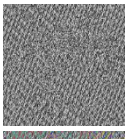
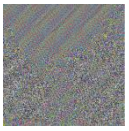
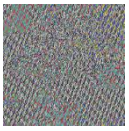
Jika koefisien korelasi sama dengan satu, itu berarti *plainimage* dan *cipherimage* adalah identik. Jika korelasi koefisien sama dengan nol, itu berarti *cipherimage* benar-benar berbeda dari *plainimage* (yaitu enkripsi yang baik) [3].

3. Hasil dan Pembahasan

Proses enkripsi dilakukan dengan menggunakan dua perlakuan. Perlakuan yang pertama yaitu enkripsi citra menggunakan *Electronic Code Book* (ECB). Citra akan dienkripsi dengan kunci yang diulang sepanjang citra yang akan dienkripsi. Proses dekripsi juga terdiri dari dua perlakuan, sama seperti pada proses enkripsi. Dimana langkah-langkah pada proses dekripsi kebalikan dari langkah-langkah yang ada pada proses enkripsi. Proses dekripsi menggunakan *Electronic Code Book* (ECB) berhasil mengembalikan *cipherimage* kedalam bentuk citra aslinya (*plainimage*). Proses enkripsi dekripsi citra menggunakan *Electronic Code Book* (ECB) dan proses enkripsi dekripsi citra menggunakan modifikasi *Electronic Code Book* (ECB) juga berhasil diterapkan melalui program MATLAB R2015a sesuai dengan metode yang diajukan oleh penulis.

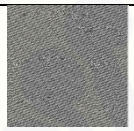
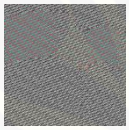
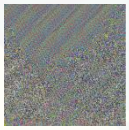
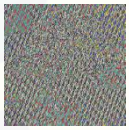
a. Enkripsi dan Dekripsi

Tabel 1. Hasil enkripsi pada program

Data Penelitian	*Plain Image*	*Cipher Image* ECB	*Cipher Image* Modifikasi ECB	Data Penelitian	*Plain Image*	*Cipher Image* ECB	*Cipher Image* Modifikasi ECB
Citra 1				Citra 5			
Citra 2				Citra 6			
Citra 3				Citra 7			
Citra 4				Citra 8			

Tabel 1 merupakan hasil dari proses enkripsi menggunakan *Electronic Code Book* (ECB), jika pixel pada *plainimage* bernilai sama, maka hasil enkripsi *pixel* pada *cipherimage* selalu bernilai sama. Sehingga hasil dari enkripsi masih terlihat polanya dan mudah untuk diduga citra aslinya. Perlakuan yang kedua, yaitu enkripsi citra menggunakan modifikasi *Electronic Code Book* (ECB). Pada proses enkripsi ini terdapat 2 tambahan operasi XOR setelah proses enkripsi *Electronic Code Book* (ECB), yaitu yang pertama diXOR-kan dengan kunci MSB dan yang kedua diXOR-kan dengan kelipatan kuncinya. Sama seperti pada enkripsi menggunakan *Electronic Code Book* (ECB), banyak kelipatan kunci harus sepanjang *plainimage*. Proses enkripsi menggunakan modifikasi *Electronic Code Book* (ECB), pixel pada *plainimage* yang bernilai sama jika di enkripsi hasilnya tidak selalu bernilai sama. Sehingga citra yang dihasilkan terlihat acak (tidak berpola).

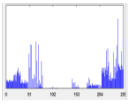
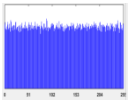
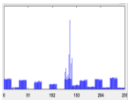
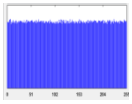
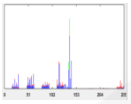
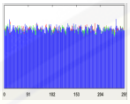
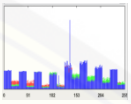
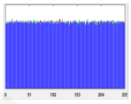
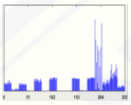
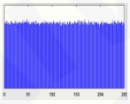
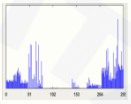
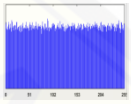
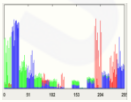
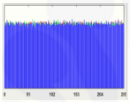
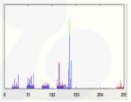
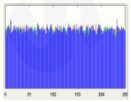
Tabel 2. Hasil dekripsi pada program

Data Penelitian	*Cipher Image* ECB	*Cipher Image* Modifikasi ECB	*Plain Image*	Data Penelitian	*Cipher Image* ECB	*Cipher Image* Modifikasi ECB	*Plain Image*
Citra 1				Citra 5			
Citra 2				Citra 6			
Citra 3				Citra 7			
Citra 4				Citra 8			

Tabel 2 merupakan hasil dari proses dekripsi menggunakan *Electronic Code Book* (ECB) berhasil mengembalikan cipher image ke dalam bentuk citra aslinya (plain image). Pada perlakuan kedua, yaitu proses dekripsi citra menggunakan modifikasi *Electronic Code Book* (ECB) dimulai dengan 2 operasi XOR sebelum proses dekripsi *Electronic Code Book* (ECB), yaitu yang pertama diXOR-kan kelipatan kuncinya dan yang kedua diXOR-kan dengan kunci MSB. Sama seperti pada dekripsi menggunakan *Electronic Code Book* (ECB), banyak kelipatan kunci harus sepanjang *cipherimage*. Sehingga hasil yang diperoleh dari proses dekripsi menggunakan kedua perilaku tersebut, berhasil mengembalikan *chiper image* menjadi *plainimage* awal. Proses dekripsi citra menggunakan *Electronic Code Book* (ECB) dan proses dekripsi citra menggunakan modifikasi *Electronic Code Book* (ECB) juga berhasil diterapkan melalui program MATLAB R2015a sesuai dengan metode yang diajukan oleh penulis.

Analisis Histogram

Tabel 3. Hasil analisis histogram

Data Penelitian	ECB	Modifikasi ECB	X^2	Data Penelitian	ECB	Modifikasi ECB	X^2
Citra 1			ECB : 603640,78 Modifikasi ECB : 550,75	Citra 5			ECB : 3513578,13 Modifikasi ECB : 769,92
Citra 2			ECB : 2676826,47 Modifikasi ECB : 572,52	Citra 6			ECB : 970337,48 Modifikasi ECB : 749,33
Citra 3			ECB : 2374031,62 Modifikasi ECB : 539,25	Citra 7			ECB : 603640,78 Modifikasi ECB : 550,75
Citra 4			ECB : 2807411,36 Modifikasi ECB : 792,63	Citra 8			ECB : 2676826,47 Modifikasi ECB : 572,52

Tabel 3 menghasilkan histogram yang lebih seragam menggunakan modifikasi *Electronic Code Book* (ECB) dibandingkan hasil histogram yang hanya menggunakan *Electronic Code Book* (ECB), terlihat juga dari perhitungan X^2 bahwa hasil yang diperoleh modifikasi *Electronic Code Book* (ECB) lebih kecil dibandingkan perhitungan yang dihasilkan menggunakan *Electronic Code Book* (ECB), itu artinya hasil dari proses enkripsi dengan metode modifikasi *Electronic Code Book* (ECB) akan lebih kuat terhadap serangan kriptanalisis dibandingkan dengan metode yang hanya menggunakan *Electronic Code Book* (ECB).

b. Hasil analisis diferensial menggunakan *Electronic Code Book* (ECB) dan menggunakan Modifikasi *Electronic Code Book* (ECB).

Berdasarkan teori analisis diferensial, batas minimal indikator NPCR sebesar 99,609375% dan batas minimal UACI sebesar 33,463541%. Berdasarkan hasil yang telah diperoleh bahwa hasil dari nilai NPCR dan UACI modifikasi *Electronic Code Book* (ECB) pada Tabel 4 sebagian besar lebih mendekati batas minimal dari indikator dibandingkan dengan *Electronic Code Book* (ECB). Hasil nilai NPCR dan UACI *Electronic Code Book* (ECB) lebih baik dibandingkan dengan hasil nilai NPCR dan UACI modifikasi *Electronic Code Book* (ECB). Secara numerik, *Electronic Code Book* (ECB) lebih baik daripada modifikasi *Electronic Code Book* (ECB), tetapi secara visual hasil dari enkripsi modifikasi *Electronic Code Book* (ECB) lebih baik dari *Electronic Code Book* (ECB) karena citra yang dihasilkan oleh modifikasi *Electronic*

Code Book (ECB) terlihat acak (tidak berpola). Tidak berkorelasinya antara uji numerik dengan tampilan visual karena uji diferensial kurang baik pada kasus ini.

Tabel 4. Hasil analisis diferensial (1)

No.	Data Penelitian	NPCR		UACI	
		ECB	Modifikasi ECB	ECB	Modifikasi ECB
1.	Citra 1	100%	99,6341%	36,0299%	30,2821%
2.	Citra 2	100%	99,6163%	55,7015%	41,7557%
3.	Citra 3	100%	99,6089%	32,5180%	29,7142%
4.	Citra 4	100%	99,6109%	39,9752%	31,3152%
5.	Citra 5	100%	99,6109%	39,8961%	34,9454%
6.	Citra 6	100%	99,6109%	37,2973%	33,5957%
7.	Citra 7	100%	99,6102%	23,1463%	28,7809%
8.	Citra 8	100%	99,6091%	29,8186%	30,1928%

Hasil dari analisis diferensial juga menghasilkan data seperti Tabel 5, dimana pada kolom ketiga dan kelima merupakan hasil perhitungan NPCR dan UACI yang diperoleh dari perhitungan antara citra hasil dari proses dekripsi dan *plainimage* menggunakan Modifikasi *Electronic Code Book* (ECB), pada kolom keempat dan keenam merupakan hasil perhitungan NPCR dan UACI yang diperoleh dari perhitungan antara citra hasil dari proses dekripsi dan *plainimage* menggunakan Modifikasi *Electronic Code Book* (ECB).

Tabel 5. Hasil analisis diferensial (2)

No.	Data Penelitian	NPCR		UACI	
		ECB	Modifikasi ECB	ECB	Modifikasi ECB
1.	Citra 1	0 %	0 %	0 %	0 %
2.	Citra 2	0 %	0 %	0 %	0 %
3.	Citra 3	0 %	0 %	0 %	0 %
4.	Citra 4	0 %	0 %	0 %	0 %
5.	Citra 5	0 %	0 %	0 %	0 %
6.	Citra 6	0 %	0 %	0 %	0 %
7.	Citra 7	0 %	0 %	0 %	0 %
8.	Citra 8	0 %	0 %	0 %	0 %

c. Hasil analisis koefisien korelasi menggunakan *Electronic Code Book* (ECB) dan Modifikasi *Electronic Code Book* (ECB).

Data-data dalam kolom ketiga pada Tabel 6 merupakan hasil perhitungan koefisien korelasi yang diperoleh dari perhitungan antara *plainimage* dan *cipherimage* menggunakan *Electronic Code Book* (ECB), kemudian data-data dalam kolom keempat

merupakan hasil dari perhitungan koefisien korelasi yang diperoleh dari perhitungan antara *plainimage* dan *cipherimage* menggunakan Modifikasi *Electronic Code Book* (ECB), sedangkan data-data yang ada pada kolom kelima adalah hasil analisis koefisien korelasi antara citra hasil dekripsi dengan *plainimage* awal.

Tabel 6. Hasil analisis koefisien korelasi

No.	Data Penelitian	ECB	Modifikasi ECB	Dekripsi
1.	Citra 1	0,00092494	0,00059775	1
2.	Citra 2	-0,38544	0,00064497	1
3.	Citra 3	-0,076992	0,00127050	1
4.	Citra 4	-0,16165	0,00022497	1
5.	Citra 5	-0,20538	0,00072037	1
6.	Citra 6	-0,16679	0,00082828	1
7.	Citra 7	0,011124	0,00012569	1
8.	Citra 8	0,061347	0,00010338	1

Citra aman dalam serangan statistik apabila dengan mengukur korelasi antara *plainimage* dan *cipherimage* hasilnya sama dengan nol atau mendekati nol. Begitu sebaliknya, apabila koefisien korelasi sama dengan satu, itu berarti *plainimage* dan *cipherimage* adalah identik dan mudah diserang oleh serangan statistik. Pada Tabel 6 dapat dilihat bahwa semua hasil nilai koefisien korelasi menggunakan modifikasi *Electronic Code Book* (ECB) mendekati nol dan lebih kecil dibandingkan dengan nilai koefisien korelasi menggunakan *Electronic Code Book* (ECB), itu artinya modifikasi *Electronic Code Book* (ECB) lebih kuat terhadap serangan statistik dibandingkan dengan *Electronic Code Book* (ECB). Hasil dari analisis koefisien korelasi terhadap hasil dekripsi dengan *plainimage* pada Tabel 6 juga menunjukkan nilai 1, itu artinya citra hasil dekripsi sangat identik dengan *plainimage* awal dan dapat dikatakan juga bahwa proses dekripsi berhasil mengembalikan *cipherimage* ke *plainimage* awal.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa:

a. Proses enkripsi menggunakan *Electronic Code Book* (ECB) menghasilkan *cipherimage* yang masih terlihat polanya, sehingga kurang aman dalam serangan kriptanalisis. Proses dekripsi citra menggunakan *Electronic Code Book* (ECB) dapat dapat mengembalikan *cipherimage* kedalam citra aslinya.
b. Proses enkripsi citra menggunakan Modifikasi *Electronic Code Book* (ECB) dapat menghasilkan *cipherimage* yang terlihat acak, sehingga aman dalam serangan kriptanalisis. Proses dekripsi citra menggunakan Modifikasi *Electronic Code Book* (ECB) dapat mengembalilkan *cipherimage* kedalam citra aslinya.

c. Berdasarkan perbandingan antara hasil perhitungan dari histogram, NPCR, UACI, dan koefisien korelasi. Tingkat keamanan hasil penyandian citra menggunakan Modifikasi *Electronic Code Book* (ECB) menghasilkan nilai yang lebih mendekati batas indikator aman, sehingga dapat disimpulkan bahwa penyandian citra menggunakan Modifikasi *Electronic Code Book* (ECB) lebih kuat dibandingkan dengan hasil penyandian citra menggunakan *Electronic Code Book* (ECB).

Daftar Pustaka

[1] Boriga, R. E., Dăscălescu, A. C. dan Diaconu, A. V. (2014). A New Fast Image Encryption Scheme Based on 2D Chaotic Maps. *IAENG International Journal of Computer Science*, 41(4): 1-10.

[2] Gabriel. (2012). An enhanced Least Significant Bit Steganographic Method for Information Hiding. *Journal of Information Engineering and Applications* Vol 2 No.9.

[3] Mousa, A., Allah, O. S. F. dan Nigm, E. S. M. (2013). Security Analysis of Reverse Encryption Algorithm for Databases. *International Journal of Computer Applications* (0975 – 8887), 66(14): 19-27.

[4] Mufid, A. (2010). Teknik Enkripsi dan Deskripsi Menggunakan Algoritma *Electronic Code Book* (ECB). *Jurnal Teknik*, 6(1): 21 – 25.