Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Penerapan Algoritma Blok Cipher Oe-Ck (Odd-Even Confusing Key) Pada Aplikasi Pengamanan Gambar

Lasma Hutagaol
Fakultas Ilmu Komputer, Teknik Informatika, Universitas Budidarma, Medan, Indonesia
Email: lasmahutagaol12@gmail.com
Email Penulis: lasmahutagaol12@gmail.com

Abstrak− Dalam kriptografi, enkripsi dan dekripsi, enkripsi merupakan proses mengamankan data gambar asli menjadi gambar yang tidak dapat dimengerti, sedangkan dekripsi merupakan proses mengembalikan data gambar yang telah di enkripsi agar mudah dibaca. Dalam proses enkripsi dan dekripsiterdapat key kunci) yang fungsinya sebagai jembatan antara enkripsi dan dekripsi dalam mendukung kekuatan pengamanan gambar.Berdasarkan atas permasalahan tersebut penulis akan membuat sebuah proses pengamanan gambar dalam bentuk citra dapat dilakukan dalam mengenkripsi citra kedalam bentuk algoritma tertentu. Ini dimungkinkan mengingat sebuah citra dapat dipresentasikan dalam sebuah tabel yang berisi bilangan-bilangan biner.Pada penelitian ini Algoritma blok cipher OE-CK akan diimplementasikan untuk menyandikan citra dengan format jpeg, yang mempunyai ukuran 1000x1200 piksel. Kunci yang digunakan untuk menyandikan citra menggunakan kunci yaitu “Lasma Hutagaol”..

Kata Kunci: Ganjil-genap Tombol Membingungkan, citra, Kanan, Kiri

Abstract−In cryptography, encryption and decryption, encryption is the process of securing the original image data into an incomprehensible image, while decryption is the process of returning encrypted image data so that it is easy to read. In the process of encryption and decryption there is a key which functions as a bridge between encryption and decryption in supporting the strength of image security. Based on these problems the author will make a process of securing images in the form of images that can be carried out in encrypting images into certain algorithm forms. This is possible considering that an image can be represented in a table containing binary numbers. In this study the OE-CK block cipher algorithm will be implemented to encode images in jpeg format, which has a size of 1000x1200 pixels. The key used to encode the image uses the key "Lasma Hutagaol".

Keywords: Odd-even Confusing Key, imagery, Right, Left..

1. PENDAHULUAN

Keamanan merupakan salah satu hal yang telah menjadi kebutuhan terpenting dalam proses berkomunikasi. Komunikasi dilakukan dengan tujuan menyampaikan informasi baik informasi bersifat penting maupun tidak penting. Pengamanan terhadap informasi tersebut tetap utuh dan terjamin. Seringkali informasi dalam bentuk gambar yang sifatnya rahasia dengan mudahnya dapat diketahui, dimodifikasi dan disalahgunakan oleh pihak-pihak yang lain.
Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi [1].
Salah satu metode pengamanan untuk tujuan di atas adalah menggunakan teknik keamanan Odd-even confusing key, diantaranya adalah algoritma blok cipher odd-even confusing key. Odd-even confusing key merupakan substitusi struktur dan struktur jaringan Feistel untuk ekspansi kunci dan enkripsi atau dekripsi. Ketika struktur jaringan Feistel digunakan untuk ekspansi kunci, struktur jaringan SP digunakan untuk enkripsi atau dekripsi. Metode ini menggunakan struktur jaringan untuk melakukan tidak hanya kunci ekspansi tetapi juga enkripsi atau dekripsi; dengan demikian, ekspansi kuncinya adalah lebih maju. Struktur jaringan SP dan struktur jaringan Feistel mengandung beberapa komponen operasi yang berbeda, untuk memastikan kunci perluasan dan operasi enkripsi atau dekripsi sinkronisasi kecepatan sejauh mungkin. Kunci utama 32-bit terbaru mengambil sebagai sinyal kontrol untuk memilih satu dari dua struktur untuk mengenkripsi atau mendekripsi sementara yang lain dipilih untuk mengoperasikan ekspansi kunci. Ada 232 = 4.294.697.296 cara berbeda operasi. Bandingkan dengan struktur tetap dalam enkripsi atau dekripsi dan kunci ekspansi, metode enkripsi yang diusulkan dapat meningkatkan kekebalan [2]..

2. METODOLOGI PENELITIAN

2.1 Penerapan

Penerapan merupakan suatu proses bentuk tindakan yang dapat melakukan atau menginplementasikan algoritma di dalam merancang suatu aplikasiyang dapat digunakan untuk membantu pengguna dalam menyelesaikan pekerjaan yang berhubungan dengan komputerisasi. Pengertian implementasi adalah dapat dikatakan bahwa implementasi tersebut adalah bukan sekedar aktivitas, melainkan suatu kegiatan yang terencana dan dilakukan secara sungguh-sungguh berdasarkan acuan norma tertentu untuk mencapai tujuan kegiatan atau pemanfaatan dan juga untuk perihal mempraktikan[3].

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

2.2 Gambar

Citra adalah gambar dua dimensi yng dihasilkan dari gambar analog dua dimensi yang continue menjadi gambar diskit melalui proses sampling. Setiap elemen pada citra dibentuk dari pixel-pixel. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwasebuah warna merupakan kombinasi dari tiga warna dasar yaitu Red, Green, Blue. Gambar juga bisa menjadi sebuah ekspresi perasaan oleh pembuatnya yang suka atau gemar untuk menggambar dan biasanya hal itu adalah untuk menunjukkan ekspresi perasaan pada gambar yang dia buat[4]. Oleh , karena hal itu gambar adalah termasuk jugamenjadi karya seni yang membutuhkan keahlian khusus untuk menghasilkan sebuah karya yang bernilai seni tinggi.Fungsi dari sebuah gambar adalah sebagai penyampaian sebuah ekspresi perasaan, sebagai media penyampaian sebuah informasi, sebagai karya seni dan dan berbagai fungsi lainnya.

2.3 Kriptografi

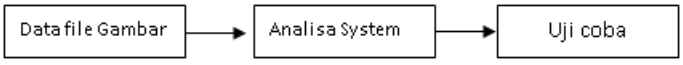
Kriptografi (chriptography) berasal dari bahasa yunani, yaitu dari kata Cryptodan graphia yang berarti "penulisan rahasia". Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (cryptology). Kriptografi juga merupakan studi terhadap teknik matematis yng terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi dan ketiadaan penyangkalan[5]

2.4 Algoritma Odd-even Confusing Key

Di era perkembangan teknologi informasi saat ini, enkripsi pesan sangat dibutuhkan untuk menjaga keamanan dalam berbagai informasi antar komunikan. Enkripsi harus dibuat serumit mungkin agar sulit untuk dipecahkan oleh penyerang. Algoritma ini adalah algoritma yang bekerja pada blok 128-bit dengan kunci 128-bit. Algoritma ini menggunakan struktur feistel dengan memanfaatkan operasi substitusi, pergeseran dan pengacakan fungsi f. Untuk meningkatkan kerumitan, fungsi ekspansi kunci juga memanfaatkan aturan bit ganjil, genap dan pengacakan. Algoritma ini dirancang sedemikian rupa untuk memenuhi prinsip Confussion dan Diffusion[7]

2.5 Analisa Pengamanan Gambar

Masalah yang akan dianalisa adalah bagaimana melakukan pengamanan suatu file gambar dengan melakukan proses pengecekan atau perbandingan suatu file gambar yang asli dengan file gambar yang telah dirubah. File gambar merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain disimpan didalam sistem file yang dapat diakses dan diatur oleh pengguna. Dalam hal kejahatan file gambar biasanya dimanipulasi untuk menghilangkan bukti-bukti yang ada didalamnya, oleh sebab itu diperlukan analisis forensik untuk dapat mengamankan file gambar tersebut.
Adanya perubahan yang mengalami perubahan dari bentuk aslinya adalah berupa foto,nama,tanda tangan. Perubahan tersebut dapat diklasifikasikan sebagai tindakan sengaja atau tidak sengaja. Perubahan yang disengaja memiliki tujuan yang jahat dengan memodifikasikan konten atau menghapus hak cipta. Disamping itu, perubahan yang tidak disengaja merupakan konsekuensi dari proses operasional digital, seperti memperbaiki kecerahan, perubahan format,pengurangan ukuran,dll. Untuk membedakan file gambar yang asli atau yang sudah dirubah maka diperlukan pendeteksian terhadap file gambar tersebut. Metode yang digunakan untuk mengamankan gambar hanya mengecek integritas dari gambar tanpa menunjukkan bagian mana pada file gambar yang telah dimanipulasi. Namun tidak dapat memberikan informasi lokasi mana yang telah dimanipulasi pada file gambar. Oleh sebab itu maka diperlukan cara mengecek keamanan suatu gambar dengan memberikan suatu kode atau metadata dari file gambar.
Untuk memudahkan analisa system maka dibuat bagan aliran analisa seperti pada gambar dibawah ini:



Gambar 1. Bagan Alir Analisa Pengamanan gambar

2.6 Analisa Pengamanan Gambar Dengan Menerapkan Algoritma Blok Cipher Odd-Even Confusing Key(OE-CK)

Mengamankan file gambar dapat dilakukan dengan menggunakan algoritma blok cipher odd-even confusing key yang digunakan untuk mengamankan gambar dengan mengecek integritas dai file gambar tanpa menunjukkan bagian mana pada file gambar yang telah dimanipulasi. Salah satu metode yang dapat digunakan adalah dengan menerapkan fungsi Hxd. Fungsi Hxd mempunyai proses jika ia dipanggil dua kali oleh masukan yang benar-benar sama (sebagai misal, string yang mengandung sekuen karakter yang sama), maka ia haruslah memberi hasil yang sama pula. Ini adalah sebuah kontrak dalam banyak bahasa pemograman yang membolehkan pengguna melakukan override pada kesamaan morfologi dan fungsi Hxd bagi sebuah objek. Jika dua objek adalah adalah sama, maka kode hxd- nya pun sama. Menjadi hal yang sangat penting untuk menemukan sebuah elemen yang sama akan sama-sama meng-hxd ke slot yang sama. Adapun metode yang digunakan untuk mengecek keamanan gambar yaitu dengan algoritma blok cipher

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Odd-even confusing key. Adapun proses yang dilakukan untuk mengamankan sebuah gambar adalah dengan cara menyandikan kunci yang didapatkan oleh algoritma blok cipher odd-even confusing key.
Langkah-langkah Algoritma blok cipher Odd-even confusing key(OE-CK) adalah sebagai berikut:

a. Bagi pesan menjadi 2 bagian sepanjang 64 bit.
b. Ubah bagian kanan menjadi blok matriks.
c. Lakukan pembangkitan kunci untuk tiap iterasi
d. Lakukan perkalian xor antara subey dan blok matriks kanan.
e. Lakukan operasi substitusi dengan kotak S
f. Lakukan operasi pegeseran terhadap matriks.
g. Lakukan operasi pengacakan dengan kotak P.
h. Bentuk bagian kiri yang baru dengan bagian kanan lainnya dan bagian kanan baru dengan hasil operasi xor dari operasi dan bagian kiri yang awal.
i. Gabung hasil operasi dalam sebuah kesatuan 128 bit.
j. Ulangi hingga 10 kali iterasi.

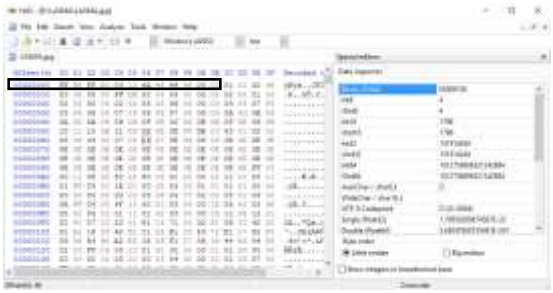
3. HASIL DAN PEMBAHASAN

3.1 Pembahasan Penerapan Algoritma OE-CK

Proses penerapan Algoritma OE-CK dilakukan sesuai dengan langkah yang sudah diuraikan pada sub bab sebelumnya. Sampel gambar yang digunakan adalah gambar dengan ekstensi JPEG. Lebih jelas dapat dilihat pada gambar berikut ini:

Gambar 2. Foto sebagai Sampel Uji Coba Algoritma OE-CK

Berikut tampilan form ekstrasi nilai piksel gambar dengan menggunakan aplikasi HxD



Gambar 3. Tampilan Nilai Hexadecimal Gambar

Nilai piksel pada gambar 3.5, yang digunakan oleh penulis sebagai sampel sebagai berikut: **FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48**

3.2. Contoh Kasus Perhitungan Algoritma OE-CK

Perhitungan Algoritma OE-CK diketahui yang menjadi pesan adalah **FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48**, nilai kunci yang digunakan "**Lasma Hutagaol**".
Langkah pertama yang dilakukan adalah proses pembentukan sub kunci berdasarkan tabel P algoritma OE-CK, sebagai berikut:

Tabel 1. Tabel P algoritma OE-CK

	1	2	3	4	5	6	7	8
1	12	6	46	11	14	50	22	33
2	20	24	19	34	63	25	9	31

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

3	29	13	54	7	47	28	32	3
4	52	53	61	40	26	41	2	43
5	35	21	39	48	27	44	45	42
6	62	55	10	36	49	58	15	5
7	37	59	38	60	0	8	16	4
8	1	17	23	18	30	56	57	51

Langkah berikutnya membuat kode sub key berdasarkan nilai kunci yang dimasukkan yaitu" **Lasma Hutagaol**", berikut tampilan lengkap tabel kode sub kunci:

Tabel 2. Tabel Kode Sub Kunci

Karakter Kunci	Binner	SubKey Kunci
L	01001100	0
a	01100001	1
s	01110011	2
m	01101101	3
a	01100001	4
	00100000	5
H	01001000	6
u	01110101	7
t	01110100	8
a	01100001	9
g	01100111	10
a	01100001	11
0	01101111	12
l	01101100	13
L	01001100	14
a	01100001	15
s	01110011	16
m	01101101	17
a	01100001	18
	00100000	19
H	01001000	20
u	01110101	21
t	01110100	22
a	01100001	23
g	01100111	24
a	01100001	25
o	01101111	26
l	01101100	27
L	01001100	28
a	01100001	29
s	01110011	30
m	01101101	31
a	01100001	32
	00100000	33
H	00100000	34
u	01110101	35
t	01110100	36
a	01100001	37
g	01100111	38
a	01100001	39
o	01101111	40
l	01101100	41
L	01001100	42
a	01100001	43
S	01110011	44
m	01101101	45
a	01100001	46
	00100000	47
H	00100000	48
u	01110101	49

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

t	01110100	50
a	01100001	51
g	01100111	52
a	01100001	53
o	01101111	54
l	01101100	55
L	01001100	56
a	01100001	57
s	01110011	58
m	01101101	59
a	01100001	60
	00100000	61
H	00100000	62
U	01110101	63

Langkah berikutnya berikutnya adalah membuat tabel kotak P untuk kunci Perubahan:

Tabel 3. Tabel Kotak P Kunci Perubahan

	1	2	3	4	5	6	7	8
1	01101111	01001000	01100001	01100001	01110101	01110100	01110100	00100000
2	01001000	01100111	00100000	01001000	00100000	01100001	01100001	01101101
3	01100001	01101100	01101111	01110101	01100111	01001100	01100001	01101101
4	01100111	01100001	00100000	01011111	01101111	01101100	01110011	01100001
5	01110101	01110101	01100001	01001000	01101100	01110011	01101101	01001100
6	01001000	01101100	01100111	01110100	01110101	01110011	01100001	00100000
7	01100001	01101101	11001111	01100001	01001100	01110100	01110011	01100001
8	01100001	01101101	01100001	01100001	01110011	01001100	01100001	01100001

Berdasarkan tabel P diatas maka nilai kunci ganjil dan kunci genap yang digunakan pada proses enkripsi OE-CK sebagai berikut:

K1 = 01101111 01001000 01100001 01100001 01110101 01110100 01110100 00100000
K2 =01001000 01100111 00100000 01001000 00100000 01100001 01100001 01101101
K3=01100001 01101100 01101111 01110101 01100111 01001100 01100001 01101101
K4= 01100111 01100001 00100000 01011111 01101111 01101100 01110011 01100001
K5=01110101 01110101 01100001 01001000 01101100 01110011 01101101 01001100
K6=01001000 01101100 01100111 01110100 01110101 01110011 01100001 00100000
K7 =01100001 01101101 11001111 01100001 01001100 01110100 01110011 01100001
K8 =01100001 01101101 01100001 01100001 01110011 01001100 01100001 01100001

Selanjutnya proses penyandian algoritma OE-CK dilakukan sebanyak 8 kali putaran. Langkah pertama bagi blok pesan menjadi dua blok yaitu Blok L *(Left)* dan Blok R *(Right)* dengan masing-masing jumlah biner perblok sebanyak 64 bit.

M = **FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48**
Hasil pembagian blok.
L0 = **FF D8 FF E0 00 10 4A 46**
R0 = **49 46 00 01 01 01 00 48**

PUTARAN 1:
Melakukan proses *fungsi round* terhadap R0:
1. Proses XOR R0 dengan Subkey K1

R0 = 01001001 01000110 00000000 00000001 00000001 00000001 00000000 01001000
K1 = 01101111 01001000 01100001 01100001 01110101 01110100 01110100 00100000
=00100110 00001110 01100001 01100000 01110100 01110101 01110100 01101000

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

2. Subtitusi biner hasil proses XOR R0 dengan Subkey K1, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Tabel 4. Kotak S untuk subtitusi nilai pada blok

Box-S OE-CK			
7	14	4	13
12	1	0	6
9	8	5	3
10	15	11	2

Tabel 5. Kotak P permutasi pesan

5, 15, 7, 2, 4, 0, 9, 8, 12, 1, 10, 14, 3, 6, 11, 13

Lakukan proses subtitusi terhadap nilai biner dari hasil proses XOR R0 dengan subkey K1 dengan cara menyusun terlebih dahulu biner kedalam bentuk matriks 4x4. Blok pertama kali diubah ke bentuk matriks 4x4 (yang berarti 1 sel berisi 4 bit pesan) untuk dioperasikan selanjutnya. Pembentukan matriks dilakukan dengan cara yang sederhana dimana pesan dibagi menjadi blok sepanjang 4 bit dan dimasukkan secara sekuensial dari kiri ke kanan pada matriks. Lebih jelasnya dapat dilihat pada tabel berikut ini:

Tabel 6. Blok Matriks Pesan

0010	0110	0000	1110
0110	0001	0110	0000
0111	0100	0111	0101
0111	0100	0110	1000

Selanjutnya dari matriks yang dihasilkan dilakukan operasi perkalian xor dengan subkey pada iterasi tersebut. Subkey juga berbentuk dalam matriks agar dapat dioperasikan.

Tabel 7. Hasil substitusi dari blok pesan matriks menggunakan kotak S

0101	1000	0100	0000
1010	0000	0110	0110
1110	1100	0010	0110
1101	1011	1101	1010

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Selanjutnya dilakukan pergeseran terhadap matriks pergeseran dilakukan terhadap sel pada matriks. Isi sel pada baris pertama dan ketiga digeser ke kanan dan baris kedua dan keempat digeser ke kiri.

Tabel 8. Hasil pergeseran blok

1010	0000	0110	0110
1101	1011	1101	1010
0101	1000	1011	0000
1110	1100	0010	0110

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Selanjutnya adalah melakukan permutasi dari hasil yang didapat dari pergeseran terhadap sel pada matriks dengan menggunakan Box-P.

Tabel 9. Pergeseran di permutasi menggunakan Box-P

1010	0000	0110	0110
10	0	6	6
1101	1011	1101	1010
13	11	13	10
0101	1000	1011	0000
5	8	11	0
1110	1100	0010	0110
14	12	2	6

Tabel 10. Permutasi

0	10	6	6
10	11	13	10
5	0	8	11
1	12	14	6

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

0000 1010 0110 0110
1010 1011 1101 1010
0101 0000 1000 1011
0001 1100 1110 0110
R0=00001010011001101010101111011010010100001000101100011100 11100110
L0=11111111 1101100011111111 11100000 00000000 00010000 01001010 01000110
R1=11110101 10111110 01010100 00111010 01010000 10011011 01010100 10100000

PUTARAN 2:
Melakukan proses *fungsi round* terhadap R1:
1. Proses XOR R1 dengan Subkey K2

R1=11110101 10111110 01010100 00111010 01010000 10011011 01010100 10100000
K2=01001000 01100111 00100000 01001000 00100000 01100001 01100001 01101101
=10111101 11011101 01110100 01110010 01110000 11111010 00110101 11001101

2. Subtitusi biner hasil proses XOR R1 dengan Subkey K2, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Tabel 11. Blok Matriks Pesan

1011	1101	1101	1101
0111	0100	0111	0010
0111	0000	1111	1010
0011	0101	1100	1101

Tabel 12. Hasil substitusi dari blok pesan matriks menggunakan kotak S

1100	0011	1001	0000
1011	0101	0111	0100
1110	1000	1010	1001
1001	1010	0111	1111

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 13. Hasil pergeseran blok

1001	1010	0111	1111
0100	1010	1001	0111
0100	0010	0000	1100
1010	0110	0101	0111

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 14. Pergeseran di permutasi menggunakan Box-P

1011	0101	0111	0100
11	5	7	4
1001	1010	0111	1111

Lanjutan **tabel 14**. Pergeseran di permutasi menggunakan Box-P

9	10	7	15
1100	0011	1001	0000
12	3	9	0
1110	1000	1010	1001
14	8	10	9

Tabel 15. Tabel Permutasi

5	7	4	11
15	7	9	10
0	9	12	3
9	8	10	14

0101 0111 0100 1011
1111 0111 1001 1010
0000 1001 1100 0011
1001 1000 1010 1110
R1=01010111 01001011 11110111 10011010 00001001 11000011 10011000 10101110

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

L1=00001010 01100110 10101011 11011010 01010000 10001011 00011100 11100110
R2 =01011101 00101101 01011100 01000000 01011001 01001000 10000100 01001000

PUTARAN 3:
Melakukan proses *fungsi round* terhadap R2:
1. Proses XOR R2 dengan Subkey K3

R2=01011101 00101101 01011100 01000000 01011001 01001000 10000100 01001000
K3=01100001 01101100 01101111 01110101 01100111 01001100 01100001 01101101
=00111100 01000001 00110011 00110101 00111110 00000100 11100101 00100101

2. Subtitusi biner hasil proses XOR R2 dengan Subkey K3, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Tabel 16. Blok Matriks Pesan

0011	1100	0100	0001
0011	0011	0011	0101
0011	1110	0000	0100
1110	0101	0010	0101

Tabel 17. Hasil substitusi dari blok pesan matriks menggunakan kotak S

0100	0010	0000	1100
1111	0010	0011	0011
1010	0110	0101	0111
0100	1010	1001	0111

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 18. Hasil pergeseran blok

1111	0010	0011	0011
0100	1010	1001	0111
0100	0010	0000	1100
1010	0110	0101	0111

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 19. Pergeseran di permutasi menggunakan Box-P

1111	0010	0011	0011
15	2	3	3
0100	1010	1001	0111
4	10	9	7
0100	0010	0000	1100
4	2	0	12
1010	0110	0101	0111
10	6	5	7

Tabel 20. Permutasi

15	2	3	3
7	4	9	10
2	4	0	12
5	7	10	14

1111 0010 0011 0011
0111 0100 1001 1010
0010 0100 0000 1100
0101 0111 1010 1110
R2=11110010 00110011 01110100 10011010 00100100 00001100 01010111 10101110
L2=01010111 01001011 11110111 10011010 00001001 11000011 10011000 10101110
R3=10100101 01111000 10000011 00000000 00101101 11001111 11001111 00000000

PUTARAN 4:
Melakukan proses *fungsi round* terhadap R3:
1. Proses XOR R3 dengan Subkey K4

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

R3=10100101 01111000 10000011 00000000 00101101 11001111 11001111 00000000
K4=01100111 01100001 00100000 01011111 01101111 01101100 01110011 01100001
=11000010 00011001 10100011 01011111 01000010 10101111 10111100 01100001

2. Subtitusi biner hasil proses XOR R3 dengan Subkey K4, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Tabel 21. Blok Matriks Pesan

1100	0010	0001	1001
1010	0011	0101	1111
0100	0010	1010	1111
1011	1100	0110	0001

Tabel 22. Hasil substitusi dari blok pesan matriks menggunakan kotak S

1011	1100	0101	0100
0110	0010	0101	1001
1101	1010	1111	1100
0001	0011	1101	0011

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 23. Hasil pergeseran blok

0110	0010	0101	1001
0001	0011	1101	0011
1011	1100	0101	0100
1101	1010	1111	1100

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 23. Pergeseran di permutasi menggunakan Box-P

0110	0001	0101	1001
6	2	5	9
0001	0011	1101	0011
1	3	11	3
1011	1100	0101	0100
11	12	5	4
1101	1010	1111	1100
11	10	15	12

Tabel 24. Permutasi

5	2	9	6
1	3	3	13
5	4	12	11
15	12	10	13

0101 0010 1001 0110
0001 0011 0011 1101
0101 0100 1100 1011
1111 1100 1010 1101
R3=01010010 10010110 00010011 00111101 01010100 11001011 111111001010 1101
L3= 11110010 00110011 01110100 10011010 00100100 00001100 01010111 10101110
R4=10100000 10100101 01100111 10100111 01110000 11000111 10101000 00000011

PUTARAN 5:
Melakukan proses *fungsi round* terhadap R4:
1. Proses XOR R4 dengan Subkey K5

R4=10100000 10100101 01100111 10100111 01110000 11000111 10101000 00000011
K5=01110101 01110101 01100001 01001000 01101100 01110011 01101101 01001100
=11010101 11010000 00000110 11101111 00011100 10000100 11000101 01001111

2. Subtitusi biner hasil proses XOR R4 dengan Subkey K5, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Tabel 25. Blok Matriks Pesan

1101	0101	1101	0000
0000	0110	1110	1111
0001	1100	1000	0100
1100	0101	0100	1111

Tabel 27. Hasil substitusi dari blok pesan matriks menggunakan kotak S

1010	1010	1001	1011
1100	0111	1110	1001
1000	0100	1101	0111
0100	1010	1111	1101

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 28. Hasil pergeseran blok

1100	0111	1110	1001
0100	1010	1111	1101
1010	1010	1001	1011
1000	0100	1101	0111

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 29. Pergeseran di Permutasi menggunakan Box-P

1100	0111	1110	1001
12	7	14	10
0100	1010	1111	1101
4	10	15	11
1010	1010	1001	1011
10	10	9	11
1000	0100	1101	0111
10	4	11	7

Tabel 30. Permutasi

7	12	10	14
15	4	10	11
9	10	10	11
7	4	10	11

0111 1100 1010 1110
1111 0100 1010 1011
1001 1010 1010 1011
0111 0100 1010 1011
R4=01111100 10101110 11110100 10101011 10011010 10101011 01110100 10101011
L4=01010010 10010110 00010011 00111101 01010100 11001011 11111100 1010 1101
R5=00101110 00111000 11100111 10010110 11001110 01100000 10001000 00000110

PUTARAN 6:
Melakukan proses *fungsi round* terhadap R5:
1. Proses XOR R5 dengan Subkey K6

R5=00101110 00111000 11100111 10010110 11001110 01100000 10001000 00000110
K6=01001000 01101100 01100111 01110100 01110101 01110011 01100001 00100000
=01100110 01010100 10000000 11100010 10111011 00010011 11101001 00100110

2. Subtitusi biner hasil proses XOR R5 dengan Subkey K6, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Tabel 31. Blok Matriks Pesan

0110	0110	0101	0100
1000	0000	1110	0010
1011	1011	0001	0011
1110	1001	0010	0110

Tabel 32. Hasil substitusi dari blok pesan matriks menggunakan kotak S

0001	1000	0001	1001
0100	0001	1110	0100
0010	0011	0100	0000
0100	0110	1001	0100

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 33. Hasil pergeseran blok

0100	0001	1110	0100
0100	0110	1001	0100
0001	1000	0001	1001
0010	0011	0100	0000

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 34. Pergeseran di permutasi menggunakan Box-P

0100	0001	1110	0100
4	1	14	4
0100	0110	1001	0100
4	6	9	4
0001	1000	0001	1001
1	8	1	9
0010	0011	0100	0000
2	3	4	0

Tabel 35. Permutasi

4	4	1	14
4	4	9	6
9	8	1	1
2	4	0	3

0100 0100 0001 1110
0100 0100 1001 0110
1001 1000 0001 0001
0010 0100 0000 0011
R5=01000100 00011110 01000100 10010110 10011000 00010001 00100100 00000011
L5=01111100 10101110 11110100 10101011 10011010 10101011 01110100 10101011
R6= 00111000 10110000 10110000 00111101 00000010 10111010 01010000 10101000

PUTARAN 7:
Melakukan proses *fungsi round* terhadap R6:
1. Proses XOR R6 dengan Subkey K7

R6=00111000 10110000 10110000 00111101 00000010 10111010 01010000 10101000
K7=01100001 01101101 11001111 01100001 01001100 01110100 01110011 01100001
=01011001 11011101 01111111 01011101 01001110 11001110 00100011 11001001

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

2. Subtitusi biner hasil proses XOR R6 dengan Subkey K7, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Tabel 36. Blok Matriks Pesan

0101	1001	1101	1101
0111	1111	0101	1101
0100	1110	1100	1110
0010	0011	1100	1001

Tabel 37. Hasil substitusi dari blok pesan matriks menggunakan kotak S

0010	0111	1001	0000
1011	1110	0101	1011
1101	0110	1001	1101
1010	1100	0111	1011

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 38. Hasil pergeseran blok

1011	1110	0101	1011
1010	1100	0111	1011
0010	0111	1001	1000
1101	0110	1001	1101

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 39 Pergeseran di permutasi menggunakan Box-P

1011	1110	0101	1011
11	14	5	11
1010	1100	0111	1011
10	12	7	11
0010	0111	1001	0000
4	7	5	0
1101	0110	1001	1101
13	6	5	13

Tabel 40. Permutasi

5	14	11	11
7	12	10	11
5	7	4	0
5	6	13	13

0101 1110 1011 1011
0111 1100 1010 1011
0101 0111 0100 0000
0101 0110 1110 1110
R6=01011110 10111011 01111100 10101011 01010111 01000000 01010110 11101110
L6=00101110 00111000 11100111 10010110 11001110 01100000 10001000 00000110
R7=01110000 10000011 10011011 00111101 10011001 00100000 11011110 11101000

PUTARAN 8:
Melakukan proses *fungsi round* terhadap R7:
1. Proses XOR R7 dengan Subkey K8

R7=01110000 10000011 10011011 00111101 10011001 00100000 11011110 11101000
K8=01100001 01101101 01100001 01100001 01110011 01001100 01100001 01100001
=00010001 11101110 11111010 01011100 11101010 01101100 10111110 10001001

2. Subtitusi biner hasil proses XOR R7 dengan Subkey K8, menggunakan Kotak S (nilainya sudah menjadi ketetapan).

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Tabel 41. Blok Matriks Pesan

0001	0001	1110	1110
1111	1010	0101	1100
1110	1010	0110	1100
1011	1110	1000	1001

Tabel 42. Hasil substitusi dari blok pesan matriks menggunakan kotak S

0110	1111	0010	0101
0011	1011	0101	1010
0111	0000	0011	1111
0001	0001	0011	1011

3. Lakukan pergeseran terhadap matriks dari hasil substitusi blok pesan

Tabel 43. Hasil pergeseran blok

0011	1011	0101	1010
0001	0001	0011	1011
0110	1111	0010	0101
0111	0000	0011	1111

4. Lakukan permutasi dari hasil pergeseran menggunakan Box-P

Tabel 44. Pergeseran di permutasi menggunakan Box-P

0011	1011	0101	1010
3	11	5	10
0001	0001	0011	1011
1	1	3	11
0110	1111	0010	0101
6	15	2	5
0111	0000	0011	1111
7	0	3	15

Tabel 45. Permutasi

5	10	3	11
1	1	3	11
15	5	2	6
15	7	0	3

0101 1010 0011 1011
0001 0001 0011 1011
1111 0101 0010 0110
1111 0111 0000 0011
R7=01011010 00111011 00010001 00111011 11110101 00100110 11110111 00000011
L7=<u>00111000 10110000 10110000 00111101 00000010 10111010 01010000 10101000</u>
R8=01100010 10001011 10100001 00000110 11110111 10011100 10100111 10101011

L7=01011010 00111011 00010001 00111011 11110101 00100110 11110111 00000011
R8=<u>01100010 10001011 10100001 00000110 11110111 10011100 10100111 10101011</u>
L8 =00111000 10110000 10110000 00111101 00000010 10111010 01010000 10101000
Maka hasil R adalah : **62 8B A1 6 F7 9C A7 AB**
Maka hasil L adalah : **38 B0 B0 3D 2 BA 50 A8**

Buletin Ilmiah Informatika Teknologi
Vol 1, No 3, Mei 2023, Hal. 83 - 96
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

4. KESIMPULAN

Dari penjelasan yang sudah diperoleh pada bab-bab sebelumnya, dapat ditarik kesimpulan bahwa:

1. Menerapkan algoritma blok cipher odd-even confusing key untuk mengamankan gambar adalah dengan memanfaatkan beberapa faslitas yang tersedia pada komputerisasi sistem, aplikasi pengamanan gambar bisa diaplikasikan dengan berbasis komputer.
2. Teknik Penerapan algoritma Odd-even Confusing Key sangat mudah mengingat proses enkripsinya menggunakan model jaringan feistel sehingga perputaran nilai cipher menghasilkan nilai cipher yang berfariasi.
3. Dengan dirancangnya aplikasi pengamanan gambar maka memudahkan pengguna aplikasi untuk menyandikan gambar atau mengembalikan ke bentuk semula.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

[1] Rifki Sadikin, Kriptografi untuk keamanan jaringan, Th. Arie Prabawati, Ed. Yogtakarta, 2012.
[2] Jurnal Informatika Mulawarman and Indah Fitri AStuti Awang Harsa Kridalaksana Fresly Nandar Pabokory, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Jurnal Informatika Mulawarman, vol. 10, p. 21, 1 Februari 2015.
[3] Kamus Besar Bahasa Indonesia Daring. Online. [Online]. https://kbbi.kemdikbud.go.id/entri/penerapan
[4] Indah Fitri Astuti Awang Harsa Kridalaksana Fresly Nandar Prabokory, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File, Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard ," Jural Informatika Mulawarman, vol. 10, p. 21, 1 Februari 2015.
[5] M.Kom Emy Setyaningsih S.Si., Kriptografi & Implementasinya Menggunakan MATLAB, Nikodemus WK, Ed. Yogyakarta, Indonesia: Andi Ed, 2015.
[6] Rinaldi Munir, Kriptografi. Bandung, Indonesia: Informatika Bandung, Oktober 2006.
[7] Aditio Pangestu Ali Akbar, "Sekolah Teknik Elektro Dan Informatika Institut Teknologi Bandung," Algoritma Blok Cipher OE-CK, 2018.
[8] Andi Juansyah, "Pembangunan Aplikasi Child Tracker Berbasis Assisted-Global Positioning System (A-GPS) Dengan Platform Android," Jurnal Ilmiah Komputer Dan Informatika, vol. 1, p. 2, 1 Agustus 2015.
[9] Rosa A.S-M.Shalahuddin, Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek). Bandung, Indonesia, 2011.
[10] S.T.,M.Eng.Sc.,Ph.D. Marwan, Belajar Mudah MATLAB Beserta Aplikasinya, Yeskha M.M., Ed. Yogyakarta Andi, Indonesia, 2017.A. Karim, S. Esabella, T. Andriani, and M. Hidayatullah, “Penerapan Metode Multi-Objective Optimization on the Basis of Simple Ratio Analysis (MOOSRA) dalam Penentuan Lulusan Mahasiswa Terbaik,” vol. 4, no. 1, pp. 162–168, 2022, doi: 10.47065/bits.v4i1.1630.
[11] N. Oktari, D. P. Utomo, S. Aripin, and A. Karim, “Penerapan Metode Operational Competitiveness Rating Analysis (OCRA) Dalam Penerimaan Karyawan Perjanjian Kerja Waktu Tertentu (PKWT),” vol. 3, no. 3, pp. 218–226, 2022, doi: 10.47065/josh.v3i3.1471.
[12] A. Karim, S. Esabella, M. Hidayatullah, and T. Andriani, “Sistem Pendukung Keputusan Aplikasi Bantu Pembelajaran Matematika Menggunakan Metode EDAS,” vol. 4, no. 3, 2022, doi: 10.47065/bits.v4i3.2494.
[13] M. Bobbi, K. Nasution, S. Suryadi, and A. Karim, “Sistem Pendukung Keputusan Dalam Rekomendasi Kelayakan nasabah Penerima Kredit Menerapkan Metode MOORA dan MOOSRA,” vol. 4, no. 3, pp. 1284–1292, 2022, doi: 10.47065/bits.v4i3.2610.