Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

Implementasi Metode Skipjack Untuk Mengamankan Citra Digital

Riki Pardede

Fakultas Ilmu Komputer Dan Teknologi Informasi, Tenik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: pardede.riki@gmail.com

Abstrak−Pengambilan gambar di setiap momen merupakan hal yang sudah sangat sering terjadi, namun tidak semua gambar yang kita ambil dapat atau ingin kita publikasikan ke media sosial, hal tersebut dikarenakan beberapa faktor yang kita anggap pribadi, maka dari itu diperlukan suatu cara untuk membantu menyamarkan atau mengacak informasi visual yang terdapat pada sebuah citra sehingga informasi tersebut hanya dapat diketahui oleh orang yang berwenang saja. Kriptografi berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data. Kriptografi memiliki banyak teknik, diantaranya adalah skipjack. Metode ini dapat digunakan untuk mengamankan gambar. Metode Skipjack merupakan suatu metode yang sederhana dimana implementasinya tidak memerlukan perhitungan-perhitungan yang rumit dan hanya melibatkan 2 buah operasi matematik kriptografi yaitu XOR dan Permutasi.

Kata Kunci: Kriptografi, Metode Skipjack, Citra Digital.

Abstract−Taking pictures at every moment is something that happens very often, but not all the pictures we take can or we want to publish to social media, this is due to several factors that we consider personal, therefore we need a way to help disguise or scramble visual information contained in an image so that the information can only be known by authorized people. Cryptography deals with aspects of information security, such as data confidentiality. Cryptography has many techniques, one of which is skipjack. This method can be used to secure images. The Skipjack method is a simple method where its implementation does not require complicated calculations and only involves 2 cryptographic mathematical operations, namely XOR and Permutation.

Keywords: Cryptography, Skipjack Method, Digital Image.

1. PENDAHULUAN

Kamera adalah alat paling popular dalam aktivitas fotografi. Kamera berawal dari sebuah alat serupa yang dikenal *camera obscura,* Bahasa latin untuk "ruang gelap", yang merupakan kotak kamera yang belum dilengkapi dengan film untuk menangkap gambar atau bayangan. Hingga saat ini kamera sudah dilengkapi dengan kemampuan untuk mengolah citra dalam bentuk digital atau yang biasa disebut dengan kamera digital [1]. Dengan adanya kamera digital ini membuat kegiatan fotografi menjadi lebih mudah, hasil tangkapan dari kamera yang kurang bagus dapat langsung dihapus atau dapat dimanipulasi untuk mendapatkan efek dari foto dengan warna yang lebih tajam. Sekarang ini banyak sekali perangkat seluler yang dilengkapi dengan kamera yang canggih, sehingga membantu setiap individu untuk mengabadikan peristiwa yang terjadi dalam hidupnya. Tidak semua hasil tangkapan foto yang diambil dapat dipublikasi ke social media, ada juga foto yang bersifat pribadi dan tidak untuk dikonsumsi publik, dan sangat merugikan jika foto tersebut jatuh ke tangan orang yang tidak berwenang. Untuk mengatasi hal ini diperlukan suatu cara yang dapat mencegah kejadian kejadian tersebut salah satu cara yang dapat digunakan adalah dengan menyamarkan atau mengacak informasi visual yang terdapat pada citra tersebut. Dengan menggunakan teknik kriptografi dapat membantu untuk menyamarkan atau mengacak informasi visual yang terdapat pada sebuah citra sehingga informasi tersebut hanya dapat diketahui oleh orang yang berwenang saja.

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*). Kriptografi juga merupakan ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, dan *integritas* data serta *autentifikasi* data. Berdasarkan jenis kunci yang digunakan, kriptografi terbagi atas dua metode, yaitu kriptografi kunci *simetris* dan kriptografi kunci *asimetris*. Perbedaan antara ke dua algoritma ini terletak pada penggunaan kunci. Untuk kriptografi kunci *simetri* menggunakan kunci yang sama pada saat melakukan *enkripsi* dan *dekripsi*. Oleh sebab itu maka harus dijaga kerahasiaannya, namun berbeda dengan kriptografi kunci *asimetris* yang menggunakan kunci yang berbeda saat melakukan *enkripsi* dan *dekripsi*, hal ini menjadi salah satu faktor kriptografi *asimetris* lebih aman dibandingkan dengan kriptografi *simetris*[2].

Algoritma *Skipjack* merupakan salah satu metode pengamanan data yang dikembangkan oleh *National Security Agency (NSA)* di Amerika Serikat yang digunakan untuk menjamin keamanan dan privasi komunikasi via telepon dan dipublikasikan pada 1998. Metode *Skipjack* merupakan suatu metode yang sederhana dimana implementasinya tidak memerlukan perhitungan-perhitungan yang rumit dan hanya melibatkan 2 buah operasi matematik kriptografi yaitu XOR dan Permutasi. Dari evaluasi yang yang dilakukan oleh para pakar atas undangan pemerintah Amerika Serikat ditemukan beberapa kehandalan metode *Skipjack* yaitu, Resiko kalau metode *Skipjack* dapat dibobol melalui metode potong kompas (cara pintas / *shortcut method*) adalah sangat kecil, selain itu juga Walaupun struktur internal algoritma *Skipjack* dirahasiakan, kekuatan *Skipjack* terhadap usaha-usaha analisis kriptografi (*cryptanalysis*) tidak bergantung kepada kerahasiaan algoritmanya [3].

Algoritma *Skipjack* memiliki kunci 80-bit yang dikenal sebagai *cryptovariable*, untuk *mengenkripsi* atau *mendekripsi* blok data 64-bit. Dalam proses *enkripsi* dan *dekripsinya Skipjack* memiliki 32 putaran yang artinya algoritma utamanya diputar sebanyak 32 kali ataupun diputar sebanyak 32 ronde untuk menghasilkan *cipherimage* ataupun gambar acak. Sehingga kombinasi dari 32 putaran atau ronde tersebut membuat algoritma *Skipjack* memiliki tingkat keamanan yang tinggi. Akan tetapi, algoritma *Skipjack* telah memiliki *kriptanalisis* yang membuat pihak ke tiga atau pihak yang ingin melihat gambar dapat mengetahuinya[4].

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yang terdiri dari kata *cryptos* yang artinya rahasia dan *graphein* yang artinya menulis. Sehingga kata kriprtografi dapat diartikan menjadi "penulisan rahasia". Kriptografi adalah ilmu yang membahas tentang teknik *enkripsi* yang mana data tersebut telah diubah susunanya menggunakan kunci sehingga data tersebut menjadi sulit untuk dibaca oleh orang lain yang tidak memiliki kunci tersebut [2]. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian *modern* kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otentikasi entitas. Berikut ini adalah rangkuman beberapa mekanisme yang berkembang pada kriptografi *modern* [6]:

a. Fungsi *Hash* adalah fungsi yang melakukan pemetaan pesan dengan panjang sembarang ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap.
b. Penyandian dengan kunci *simetrik (Symmetric key encipherment)* adalah penyandianyang kunci *enkripsi* dan kunci *dekripsi* bernilai sama. Kunci pada penyandian *simetrik* diasumsikan bersifat rahasia hanya pihak yang melakukan *enkripsi* dan *dekripsi* yang mengetahui nilainya. Oleh karena itu penyandian dengan kunci *simetrik* disebut juga penyandian dengan kunci rahasia *secret key encipherment.*
c. Penyandian dengan kunci *asimetrik (Asymmetric key encipherment)* atau sering juga disebut dengan penyandian kunci publik *(public key)* adalah penyandian dengan kunci *enkripsi* dan *dekripsi* berbeda nilai. Kunci *enkripsi* yang juga disebut dengan kunci publik *(public key)* bersifat terbuka. Sedangkan kunci dekripsi yang disebut kunci privat *(private key)* bersifat tertutup / rahasia.

2.2 Algoritma *Skipjack*

Skipjack merupakan *cipher*-blok algoritma untuk *enkripsi* dikembangkan oleh Badan Keamanan Nasional AS (NSA). Awalnya dimaksudkan untuk digunakan dalam *chip Clipper* yang kontroversial. Selanjutnya, algoritma itu tidak diklasifikasikan dan sekarang memberikan wawasan unik ke dalam desain sandi dari sebuah agen intelijen pemerintah. *Skipjack* merupakan salah satu algoritma *simetrik* di mana *Skipjack* menggunakan kunci yang sama untuk proses *enkripsi* dan proses dekripsinya [2]. *Skipjack* memiliki blok data masukan *(Plaintext*) berukuran 64 bit yang kemudian data tersebut diubah menjadi kumpulan blok-blok data yang berukuran 64 bit yang diproses dengan kunci yang sama untuk menghasilkan *Chipertext*. Kunci yang digunakan berukuran 80 bit. Dalam proses *enkripsi* dan *dekripsinya Skipjack* memiliki 32 putaran artinya algoritma utamanya diputar sebayak 32 kali untuk menghasilkan *Chipertext*. Kombinasi dari 32 putaran tersebut membuat algoritma *Skipjack* memiliki tingkat keamanan yang tinggi [7]. Itu dirancang khusus untuk menggantikan Data *Encryption* Standard (DES). Dalam *Skipjack* terdapat beberapa istilah yang digunakan yaitu antara lain:

a. *Word* : berisi 16 bit
b. *Byte* : berisi 8 bit
c. X.Y : XOR dari X dan Y

Skipjack meng*enkripsi* data sebanyak 4 word (terdiri atas 8 byte, 1byte = 16 bit). *Skipjack* mempunyai 2 aturan diantaranya adalah *Rule* A dan *Rule* B, aturan ini digunakan secara bergantian dalam proses *enkripsi* untuk mengubah *Plaintext* menjadi *Chipertext* dan dalam proses *dekripsi* untuk mengubah *Chipertext* menjadi *Plaintext.* Terdapat dua tipe putaran dalam *skipjack cipher* yang disebut dengan *stepping rule*. Kedua tipe tersebut adalah :

Tipe A :

a. Upablok W1 di*enkripsi* dengan fungsi permutasi G yang adalah empat putaran *feistel cipher* biasa.
b. Hasil *enkripsi*nya dan nomor putaran yang bertambah dari satu sampai dengan 32, di xor dengan upablok W4.
c. Setiap upablok dirotasi W1 ke W2, W2 ke W3, W3 ke W4, dan W4 ke W1.

Tipe B :

a. Upablok W2 di-xor dengan W1 dan nomor putaran.
b. W1 di*enkripsi* dengan fungsi permutasi G.
c. Setiap upablok dirotasi W1 ke W2, W2 ke W3, W3 ke W4, dan W4 ke W1.\

Adapun proses enkripsi dan deskripsi metode ini sebagai berikut:

a. Proses *Enkripsi*

   Langkah – langkah dari *rule* A adalah sebagai berikut :

   1. Lakukan permutasi G dengan input W1k.
   2. W1k+1 merupakan hasil dari operasi XOR antara output permutasi G, W4k, dan *counter*.
   3. W2k+1 merupakan *output* dari permutasi G.
   4. W3k+1 = W2k.
   5. W4k+1 = W3k.
   6. *Counter* dan k ditambah satu.

   Langkah – langkah dari *rule* B adalah sebagai berikut :

   1. Lakukan permutasi G dengan *input* W1k.
   2. W1k+1 = W4k.

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

3. W2k+1 merupakan *output* dari permutasi G.
4. W3k+1 merupakan hasil dari operasi XOR antara W1k, W2k, dan *counter*.
5. W4k+1 = W3k.
6. *Counter* dan k ditambah satu.

b. Proses *Dekripsi*

Langkah-langkah dari *rule* A adalah sebagai berikut :

1. Lakukan permutasi G-1 dengan *input* W2k.
2. W1k-1 merupakan *output* dari permutasi G-1.
3. W2k-1 = W3k.
4. W3k-1 = W4k.
5. W4k-1= merupakan hasil dari operasi XOR antara W1k, W2k dan *counter*.
6. *Counter* dan k dikurangi satu.

Langkah – langkah dari *rule* B-1 adalah sebagai berikut :

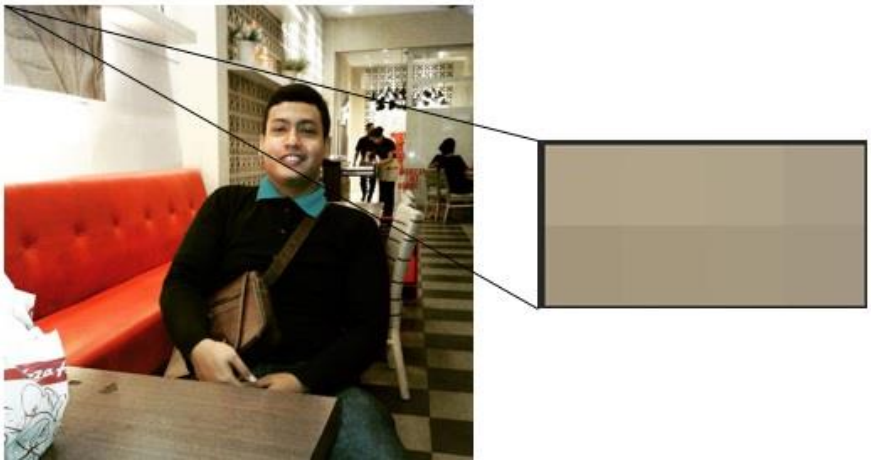
1. Lakukan permutasi G-1 dengan *input* W2k.
2. W1k-1 merupakan *output* dari permutasi G-1.
3. W2k-1 merupakan hasil dari operasi XOR antara *output* permutasi G-1, W3k, dan *counter*.
4. W3k-1 = W4k.

2.3 Citra Digital

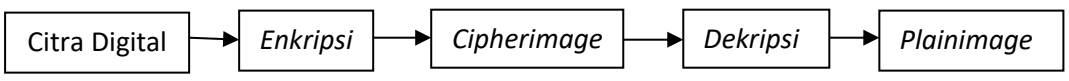
Citra adalah suatu gambaran, kemiripan atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada media penyimpanan [8]. Secara harafiah citra (image) adalah gambar pada bidang dwimatra atau dua dimensi. Citra juga dapat diartikan sebagai kumpulan titik-titik dengan intensitas warna tertentu yang membentuk suatu kesatuan dan mempunyai pengertian artistik. Citra sebagai salah satu komponen multimedia yang memegang peranan sangat penting sebagai salah satu bentuk informasi visual.

3. HASIL DAN PEMBAHASAN

Analisa masalah dilakukan untuk mendapat solusi dalam menyelesaikan permasalahan yang telah dijelaskan pada bab sebelumnya yang bertujuan untuk mencapai sistem yang baik agar mendapatkan hasil yang akurat. Adapun masalah yang diangkat penulis dalam penelitian ini adalah bagaimana mengamankan *file* video dengan menggunakan algoritma *skipjack.*



Gambar 1 *Pixel* Citra Gambar yang akan di proses



Gambar 2. Prosedur Program Citra Digital

Adapun langkah-langkah untuk mengambil nilai-nilai *pixel* citra gambar dengan matlab adalah :

a. Buka aplikasi MATLAB.
b. Siapkan gambar bertipe *jpeg* dan simpan direktori.
c. Langkah selanjutnya tuliskan *listing program*.
d. Selanjutnya akan ditampilkan nilai *pixel* yang berisikan nilai berikut ini :

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

	1	2	3	4
1	152	157	157	154
2	155	156	152	149

Gambar 3. Nilai *Pixel* Citra Gambar 2x4

Algoritma *skipjack* merupakan algoritma kriptografi dengan perputaran sebanyak 32 kali. Perputaran sebanyak 32 kali tersebut membuat algoritma *skipjack* memiliki tingkat keamanan yang sangat tinggi. Proses pengolahan kunci pada metode *skipjack* adalah proses yang dilakukan sebelum melakukan proses *enkripsi* maupun *dekripsi*. Berikut ini adalah pelaksanaan proses pengolahan kunci yang bertujuan untuk menghasilkan 10 buah subkunci (*cryptovariable*).
Kunci = RIKIPARDED
Kunci dalam bentuk hexadesimal = 52, 49, 4B, 49, 50, 41, 52, 44, 45, 44
Bagi kunci menjadi 10 subkunci (*cryptovariable*), masing-masing 8 bit sebagai berikut.
CV(0) = 52 CV(5) = 41
CV(1) = 49 CV(6) = 52
CV(2) = 4B CV(7) = 44
CV(3) = 49 CV(8) = 45
CV(4) = 50 CV(9) = 44
Proses *enkripsi* dalam metode *skipjack* memiliki 32 putaran dengan menggunakan 10 buah sub kunci yang merupakan hasil pembagian dari sebuah kunci rahasia. Berikut ini adalah proses *enkripsi* metode *skipjack* :

Desimal			
152	157	157	154
155	156	152	149
Hexadesimal			
98	9D	9D	9A
9B	9C	98	95

Gambar 4. Tabel 1 *Plainimage*

Ubahlah *plainimage* menjadi 4 bagian (W_1,W_2,W_3,W_4) sebagai berikut:
$W_1(0)$ = 989D $W_3(0)$ = 9B9C
$W_2(0)$ = 9D9A $W_4(0)$ = 9895
Putaran 1 (*Rule* A, K = 0, *Counter* = 1)
G(W1(0)) = G(989D)
g1 = 98
g2 = 9D
g3 = F(g2 ⊕ cv[(4*k) *mod* 10]) ⊕ g1
cv[(4*0) *mod* 10]) = cv[0] = 52
g2 = 9D = 1001 1101
cv[0] = 52 = 0101 0010 ⊕
1100 1111
F(1100 1111) = F(CF) = E2
F(CF) = E2 = 1110 0010
g1 = 98 = 1001 1000 ⊕
g3 = 0111 1010 (7A)
g4 = F(g3 ⊕ cv[((4*k) + 1) *mod* 10]) ⊕ g2
cv[((4*0) + 1) *mod* 10] = cv[1] = 49
g3 = 7A = 0111 1010
cv[1] = 49 = 0100 1001 ⊕
0011 0011
F(0011 0011) = F(33) = BA
F(33) = BA = 1011 1010
g2 = 9D = 1001 1101 ⊕
g4 = 0010 0111 (27)
g5 = F(g4 ⊕ cv[((4*k) + 2) *mod* 10]) ⊕ g3
cv[((4*0) + 2) *mod* 10] = cv[2] = 4B
g4 = 27 = 0010 0111
cv[2] = 4B = 0100 1011 ⊕
0110 1100

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

F(0110 1100) = F(6C) = 6D
F(6C) = 6D = 0110 1101
g3 = 7A = 0111 1010 ⊕
g5 = 0001 0111 (17)
g6 = F(g5 ⊕ cv[((4*k) + 3) *mod* 10]) ⊕ g4
cv[((4*0) + 3) *mod* 10] = cv[3] = 49
g5 = 17 = 0001 0111
cv[3] = 49 = 0100 1001 ⊕
0101 1110
F(0101 1110) = F(5E) = D8
F(5E) = D8 = 1101 1000
g4 = 27 = 0010 0111 ⊕
g6 = 1111 1111 (FF)
g5+g6 = 17FF
W1(1) = G(W1(0)) ⊕ W4(0) ⊕ *Counter*
G(W1(0)) = 17FF = 0001 0111 1111 1111
W4(0) = 9895 = 1001 1000 1001 0101 ⊕
1000 1111 0110 1010
Counter = 1 = 0000 0000 0000 0001 ⊕
1000 1111 0110 1011 [8F6B]
W2(1) = G(W1(0)) = 17FF
W3(1) = W2(0) = 9D9A
W4(1) = W3(0) = 9B9C
K = 1 ; *Counter* = 2
Cipherimage = W1(1)+W2(1)+W3(1)+W4(1) = 8F6B 17FF 9D9A 9B9C

Putaran 2 (*Rule* A, K = 1, *Counter* = 2)
G(W1(1)) = G(8F6B)
g1 = 8F
g2 = 6B
g3 = F(g2 ⊕ cv[((4*k) *mod* 10] ⊕ g1
cv[(4*1) *mod* 10]) = cv[4] = 50
g2 = 6B = 0110 1011
cv[4] = 50 = 0101 0000 ⊕
0011 1011
F(0011 1011) = F(3B) = F5
F(3B) = F5 = 1111 0101
g1= 8F = 1000 1111 ⊕
g3 = 0111 1010 (7A)
g4 = F(g3 ⊕ cv[((4*k) + 1) *mod* 10]) ⊕ g2
cv[((4*1) + 1) *mod* 10] = cv[5] = 41
g3 = 7A = 0111 1010
cv[5] = 41 = 0100 0001 ⊕
= 0011 1011
F(0011 1011) = F(3B) = F5
F(3B) = F5 = 1111 0101
g2= 6B = 0110 1011 ⊕
g4 = 1001 1110 (9E)
g5 = F(g4 ⊕ cv[((4*k) + 2) *mod* 10]) ⊕ g3
cv[((4*1) + 2) *mod* 10] = cv[6] = 52
g4 = 9E = 1001 1110
cv[6] = 52 = 0101 0010 ⊕
= 1100 1100
F(1100 1100) = F(CC) = FF
F(CC) = FF = 1111 1111
g3 7A = 0111 1010 ⊕
g5 = 1000 0101 (85)

g6 = F(g5 ⊕ cv[((4*k) + 3) *mod* 10]) ⊕ g4
cv[((4*1) + 3) *mod* 10] = cv[7] = 44
g5 = 85 = 1000 0101

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

cv[7] = 44 = 0100 0100 ⊕
= 1100 0001
F(1100 0001) = F(C1) = 04
F(C1) = 04 = 0000 0100
g4 = 9E = 1001 1110 ⊕
g6 = 1001 1010 (9A)
g5+g6 = 859A
W1(2) = G(W1(1)) ⊕ W4(1) ⊕ *Counter* 1
G(W1(1)) = 859A = 1000 0101 1001 1010
W4(1) = 9B9C = 1001 1011 1001 1100 ⊕
0001 1110 0000 0110
Counter = 2 = 0000 0000 0000 0010 ⊕
0001 1110 0000 0100 [1E04]
W2(2) = G(W1(1)) = 859A
W3(2) = W2(1) = 17FF
W4(2) = W3(1) = 9D9A
K = 2 ; *Counter* = 3
Cipherimages = W1(2)+W2(2)+W3(2)+W4(2) = 1E04 859A 17FF 9D9A
Selanjutnya hasil putaran *enkripsi* ke 3-32 ada di tabel berikut :

Tabel 1. Hasil Perhitungan *Enkripsi*

Putaran	Counter	K	W1	W2	W3	W4
3	3	2	389D	A504	859A	17FF
4	4	3	C8D6	DF2D	A504	859A
5	5	4	273C	A2A3	DF2D	A504
6	6	5	C348	664A	A2A3	DF2D
7	7	6	8446	5B6C	664A	A2A3
8	8	7	BBB7	191C	5B6C	664A
9	9	8	20E3	46A0	191C	5B6C
10	10	9	15D9	4EA5	46A0	191C
11	11	10	8476	9D7B	4EA5	46A0
12	12	11	15E7	5355	9D7B	4EA5
13	13	12	9A9B	D42D	5355	9D7B
14	14	13	AB3C	3653	D42D	5355
15	15	14	1A7D	493D	3653	D42D
16	16	15	5BC7	8FFC	493D	3653
17	17	16	4FA1	79E5	8FFC	493D
18	18	17	D751	9E74	79E5	8FFC
19	19	18	5820	D7C5	9E74	79E5
20	20	19	F698	8F5D	D7C5	9E74
21	21	20	8BA5	15F0	8F5D	D7C5
22	22	21	262A	F1CD	15F0	8F5D
23	23	22	2208	AD76	F1CD	15F0
24	24	23	6E0A	7BDE	AD76	F1CD
25	25	24	2928	D8C0	7BDE	AD76
26	26	25	C3C6	CE96	D8C0	7BDE
27	27	26	C626	BDDF	CE96	D8C0
28	28	27	85F1	5D19	BDDF	CE96
29	29	28	88C9	4676	5D19	BDDF
30	30	29	E843	55AC	4676	5D19
31	31	30	AF1E	F236	55AC	4676
32	32	31	2824	6E60	F236	55AC

Hasil dari nilai akhir *Enkripsi* pada Citra Digital (gambar) dapat dilihat sebagai berikut :
Ket : Hexadesimal (28246E60F23655AC) ubah ke Desimal (4036110962425485172)

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

Gambar 5. Hasi Enkripsi Nilai *Pixel* Citra

Proses *dekripsi* merupakan kebalikan dari proses *enkripsi*, yang bertujuan untuk mengembalikan *cipher images* kebentuk *plainimages* (karakter awal). Berikut adalah proses *dekripsi* :
Ubah *cipherimages* kedalam bentuk hexadesimal : 2824, 6E60, F236, 55AC. kemudian bagi *cipherimages* menjadi 4 bagian (W1, W2, W3, W4) yaitu sebagai berikut:
W1(32) = 2824 W3(32) = F236
W2(32) = 6E60 W4(32) = 55AC
Di bawah ini adalah hasil perhitungan *dekripsi* dari putaran 1-32 sebagai berikut :

Tabel 2. Hasil Perhitungan *Dekripsi.*

Putaran	Counter	K	W1	W2	W3	W4
1	32	32	AF1E	F236	55AC	4676
2	31	31	E843	55AC	4676	5D19
3	30	30	88C9	4676	5D19	BDDF
4	29	29	85F1	5D19	BDDF	CE96
5	28	28	C626	BDDF	CE96	D8C0
6	27	27	C3C6	CE96	D8C0	7BDE
7	26	26	2928	D8C0	7BDE	AD76
8	25	25	6E0A	7BDE	AD76	FICD
9	24	24	2208	AD76	F1CD	15F0
10	23	23	262A	F1CD	15F0	8F5D
11	22	22	8BA5	15F0	8F5D	D7C5
12	21	21	F698	8F5D	D7C5	9E74
13	20	20	5820	D7C5	9E74	79E5
14	19	19	D751	9E74	79E5	8FFC
15	18	18	4FA1	79E5	8FFC	493D
16	17	17	5BC7	8FFC	493D	3653
17	16	16	1A7D	493D	3653	D42D
18	15	15	AB3C	3653	D42D	5355
19	14	14	9A9B	D42D	5355	9D7B
20	13	13	15E7	5355	9D7B	4EA5
21	12	12	8476	9D7B	4EA5	46A0
22	11	11	15D9	4EA5	46A0	191C
23	10	10	20E3	46A0	191C	5B6C
24	9	9	BBB7	191C	5B6C	664A
25	8	8	8446	5B6C	664A	A2A3
26	7	7	C348	664A	A2A3	DF2D
27	6	6	273C	A2A3	DF2D	A504
28	5	5	C8D6	DF2D	A504	859A
29	4	4	389D	A504	859A	17FF
30	3	3	1E04	859A	17FF	9D9A
31	2	2	8F6B	17FF	9D9A	9B9C
32	1	1	989D	9D9A	9B9C	9895

Hasil dari nilai akhir *Enkripsi* pada Citra Digital (gambar) dapat dilihat sebagai berikut :
Ket : Hexadesimal (98;9D;9D;9A;9B;9C;98;95) ubah ke Desimal (152; 157; 157; 154; 155; 156; 152; 149)

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan penulis tentang implementasi metode skipjack untuk mengamankan citra digital, maka kesimpulan yang dapat diambil dimna hasil proses *enkripsi* dan *dekripsi* yang bertujuan untuk mencapai sistem yang baik agar mendapatkan hasil yang akurat. Serta hasil proses keluaran program *enkripsi* dan *dekripsi* terbukti dengan menggunakan metode *skipjack file* gambar sangat aman.

REFERENCES

[1] Hartono, "Aplikasi Pengamanan Data Menggunakan Metode Skipjack," Stmik Ibbi, no. 18, pp. 39–50, 2009.
[2] Sentot Kromodimoeljo, Teori & Aplikasi Kriptografi. SPK IT Consulting, 2010.

Jurnal Sains Dan Teknologi Informasi
Vol 1, No 1, Desember 2021, Hal 28-35
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v1i1.988
Website https://ejurnal.seminar-id.com/index.php/jussi

[3] R. S. Andi, "kriptografi untuk Keamanan Jaringan dan Impelementasinya dalam Bahasa Java," pp. 341–342, 2012.
[4] Dony Ariyus, Pengantar Ilmu Kriptografi_ Teori Analisis & Implementasi - Dony Ariyus, Universitas Amikom - Google Buku. Yogyakarta: C.V ANDI OFFSET, 2008.
[5] Y. Kurniawan, "Kriptografi, Keamanan Internet dan Jaringan Komunikasi." Informatika Bandung, Bandung, 2004.
[6] E. Setyaningsih, "Kriptografi dan Implementasinya Menggunakan Matlab," Andi, vol. 2, no. 2, pp. 151–157, 2015.
[7] . S., "SISTEM PENGKODEAN DATA PADA FILE TEKS PADA KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE SKIPJACK," J. Comput. BISNIS, vol. 1, no. 2, pp. 105–118, 2015.
[8] A. Kadir and A. Susanto, Teori dan Aplikasi Pengolahan Citra, I. Yogyakarta: CV. Andi Offset, 2013.
[9] A. Mabrur and S. Si, "Pengolahan Citra Digital Menggunakan," no. March, pp. 1–40, 2011.
[10] M. Shalahuddin and A. . Rosa, Kolaborasi Rekayasa Perangkat Lunak Terstruktur dan Berorientasi. Bandung: Informatika Bandung, 2015.