JNATIA Volume 3, Nomor 1, November 2024 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Pengamanan Gambar dengan Metode Cipher Block Chaining

Made Yayang Eka Prananda[1)], I Gusti Ngurah Anom Cahyadi Putra [2)]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]yayangp32@.gmail.com
[2]anom.cp@unud.ac.id

Abstract

Data security is something that everyone needs to maintain their privacy, for example images. Images are very familiar to everyone, because we can capture various moments in the form of images. But there are some people who steal someone's image to misuse it for personal gain. Image pixel encryption using cryptography can be an alternative in securing the image. In this study, the cipher block chaining method is used to encrypt each pixel. The results of using this method are quite satisfactory, the resulting image becomes more abstract. The encrypted image can also be decrypted into the original image. However, the resulting pattern is still the same as the previous image pattern. So the use of this method may be more effective when combined with other cryptographic methods.

Keywords: *Cipher Block Chaining, Encrypted, Decrypted, Photo, Pixel.*

1. Pendahuluan

Keamanan data merupakan suatu hal yang dibutuhkan semua orang untuk menjaga privasinya. Untuk itu banyak cara dilakukan agar privasi tersebut dapat terjaga dengan aman. Privasi seseorang dapat berupa teks, gambar maupun video. Gambar sangat familiar di dengar oleh semua orang, karena kita dapat mengabadikan berbagai momen dalam bentuk gambar. Mulai dari berlibur, bersama keluarga, bersama orang tersayang dapat kita abadikan momennya dalam bentuk gambar untuk dapat dikenang suatu hari nanti. Namun ada saja beberapa oknum yang memanfaatkan hal ini, dengan menggunakan gambar privasi untuk disalahgunakan. Seperti mengambil gambar privasi tersebut untuk disebarkan demi mendapat keuntungan tersendiri. Oleh karena itu dalam menyimpan gambar privasi kita harus bisa mengamankannya. Mengamankan gambar dapat dilakukan dengan berbagai cara, seperti menyimpan di folder tersembunyi, memberi proteksi kepada folder tempat menyimpan gambar, dan lainnya. Namun ada satu cara yang dapat memberi proteksi yang sangat tinggi, yaitu dengan mengacak acak warna gambar tersebut dengan menggunakan algoritma kriptografi. Sehingga gambar asli yang sebelumnya sangat indah menjadi gambar yang sangat tidak jelas atau abstrak. Banyak algoritma kriptografi yang sangat efisien dalam mengenkripsi setiap pixel gambar tersebut salah satunya Cipher Block Chaining. Cipher Block Chaining digunakan karena merupakan salah satu algoritma modern yang menggunakan block cipher dan dalam melakukan enkripsi menggunakan inisialisasi variabel yang saling terkait. Sehingga apabila ada salah satu pixel yang di rusak, pixel selanjutnya akan menjadi lebih tidak jelas. Diharapkan dengan menggunakan Cipher Block Chaining dalam melakukan enkripsi setiap pixel sebuah gambar, dapat membuat seseorang mengamankan gambarnya lebih aman.

2. Metode Penelitian

2.1 Algoritma Cipher Block Chaining

Menurut Menezes et al (1997) algoritma Cipher Block Chaining (CBC) merupakan salah satu metode kriptografi yang berbasis pada block, pada metode ini mempunyai kelebihan setiap block

ciphertext bergantung tidak hanya pada block plaintextnya tetapi juga pada seluruh block plaintext sebelumnya. Mode operasi Cipher Block Chaining (CBC) merupakan salah satu mode operasi block cipher yang menggunakan vektor inisialisasi (initialitation vector/IV) dengan ukuran tertentu (ukurannya sama dengan satu blok plaintext). Pada mode operasi ini plaintext dibagi menjadi beberapa blok, kemudian masing-masing blok dienkripsi dengan ketentuan blok plaintext pertama dienkripsi lebih dahulu. Sebelum dienkripsi, plaintext di-XOR dengan IV. Lalu, hasil XOR tersebut dienkripsi hingga menghasilkan ciphertext. Selanjutnya, ciphertext tersebut digunakan sebagai IV untuk proses penyandian blok plaintext selanjutnya. Algortima CBC merupakan kriptografi simetris jadi kunci digunakan dalam proses enkripsi dan juga dekripsi adalah kunci yang sama. Namun untuk enkripsi CBC memerlukan inisialisasi variabel sebagai tambahan dalam melakukan enkripsi, untuk sistematis proses enkripsi CBC dapat dilihat pada gambar 2.1. Contoh dalam melakukan proses enkripsi, yaitu:

Proses Enkripsi

Plaintext: Nan
Key: ya
IV: 01100101

Ubah plaintext dan kunci ke bentuk biner:

Plaintext
- N: 01001110
- a: 01100001
- n: 01101110

Kunci
- y: 01111001
- a: 01100001

Atur plaintext dengan tiap kunci:

Plaintext	**N**	**a**	**n**
Kunci	y	a	y

Langkah-Langkah Enkripsi:

a. **C1 diperoleh dari:**
P1⊕C0=01001110⊕01100101=00101011P1 \oplus C0 = 01001110 \oplus 01100101 = 00101011
Enkripsi hasil tersebut (C1) dengan fungsi **E**:
C1⊕K1=00101011⊕01111001=01010010C1 \oplus K1 = 00101011 \oplus 01111001 = 01010010
Geser hasilnya satu bit ke kiri: 1010010010100100

b. **C2 diperoleh dari:**
P2⊕C1=01100001⊕10100100=11000101P2 \oplus C1 = 01100001 \oplus 10100100 = 11000101
Enkripsi hasil tersebut (C2) dengan fungsi **E**:
C2⊕K2=11000101⊕01100001=10100100C2 \oplus K2 = 11000101 \oplus 01100001 = 10100100
Geser hasilnya satu bit ke kiri: 0100100101001001

c. **C3 diperoleh dari:**
P3⊕C2=01101110⊕01001001=00100111P3 \oplus C2 = 01101110 \oplus 01001001 = 00100111

Enkripsi hasil tersebut (C3) dengan fungsi **E**:
C3⊕K3=00100111⊕01111001=01011110C3 \oplus K3 = 00100111 \oplus 01111001 = 01011110
Geser hasilnya satu bit ke kiri: 1011110010111100

Hasil Enkripsi

Plaintext	Binary	Ciphertext
N	01001110	10100100
a	01100001	01001001
n	01101110	10111100

Proses Dekripsi

Ciphertext: 10100100 01001001 10111100
Key: ya
IV: 01100101

Ubah kunci ke bentuk biner:

Kunci
- y: 01111001
- a: 01100001

Langkah-Langkah Dekripsi:

a. **P1 diperoleh dari:**
Dekripsi **C1** dengan fungsi **D**:
Geser ciphertext satu bit ke kanan: 0101001001010010
C1⊕K1=01010010⊕01111001=00101011C1 \oplus K1 = 01010010 \oplus 01111001 = 00101011
Hasil dekripsi tersebut di XOR dengan C0C0:
P1⊕C0=00101011⊕01100101=01001110P1 \oplus C0 = 00101011 \oplus 01100101 = 01001110

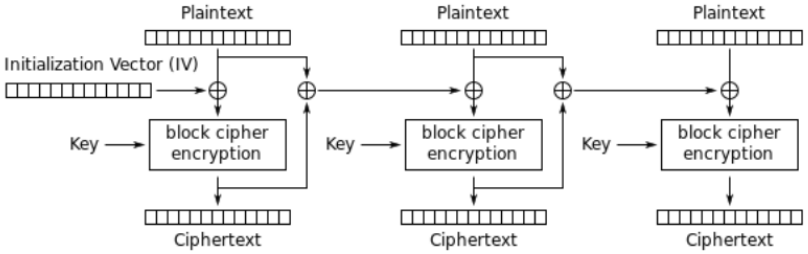
b. **P2 diperoleh dari:**
Dekripsi **C2** dengan fungsi **D**:
Geser ciphertext satu bit ke kanan: 1010010010100100
C2⊕K2=10100100⊕01100001=11000101C2 \oplus K2 = 10100100 \oplus 01100001 = 11000101
Hasil dekripsi tersebut di XOR dengan C1C1:
P2⊕C1=11000101⊕10100100=01100001P2 \oplus C1 = 11000101 \oplus 10100100 = 01100001

c. **P3 diperoleh dari:**
Dekripsi **C3** dengan fungsi **D**:
Geser ciphertext satu bit ke kanan: 0101111001011110
C3⊕K3=01011110⊕01111001=00100111C3 \oplus K3 = 01011110 \oplus 01111001 = 00100111
Hasil dekripsi tersebut di XOR dengan C2C2:
P3⊕C2=00100111⊕01001001=01101110P3 \oplus C2 = 00100111 \oplus 01001001 = 01101110

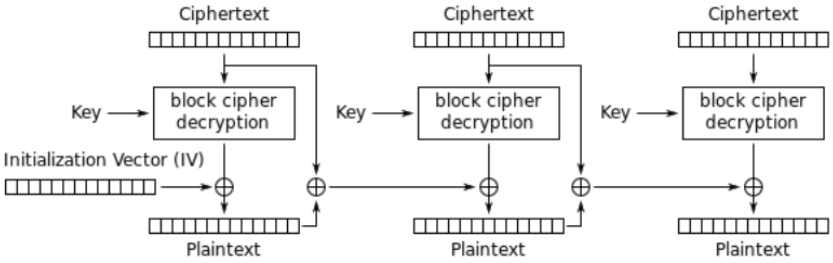
p-ISSN: 2986-3929
e-ISSN: 3032-1948

Hasil Dekripsi

Ciphertext	Binary	Plaintext
10100100	01001110	N
01001001	01100001	a
10111100	01101110	n



Gambar 2.1 Flowchart Proses Enkripsi Cipher Block Chainng

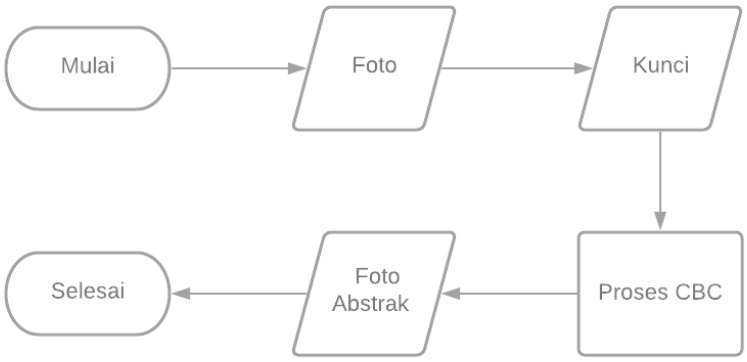


Gambar 2.2 Flowchart Proses Dekripsi Cipher Block Chaining

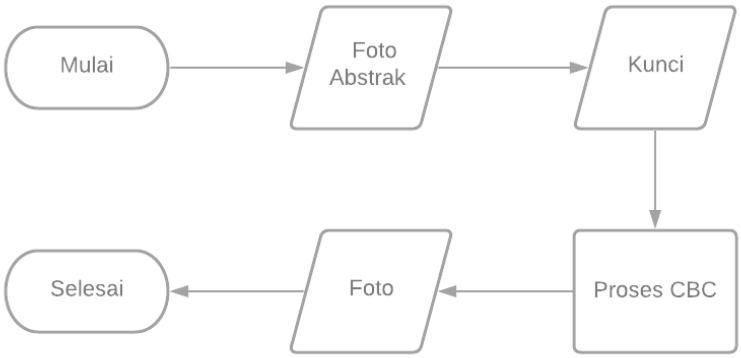
2.2 Flowchart

Pada penelitian ini, akan menggunakan Cipher Block Chaining sebagai enkripsi maupun dekripsi gambar yang ingin diamankan. Namun format gambar yang digunakan dibatasi dengan hanya menggunakan format png. Untuk proses melakukan enkripsi dimulai dengan pengguna menginput gambar dan kata sandi untuk mengenkripsi, lalu program akan melakukan enkripsi setiap pixel, outputnya berupa gambar baru yang sudah tidak terlihat jelas atau abstrak. Flowchart dalam melakukan proses enkripsi dapat dilihat pada gambar 2.3. Untuk proses melakukan dekripsi dimulai dengan pengguna menginput gambar abstrak dan kata sandi yang digunakan dalam melakukan enkripsi, lalu program akan melakukan dekripsi setiap pixel, outputnya berupa gambar privasi yang sebelumnya di enkripsi. Untuk flowchart proses dekripsi dapat dilihat pada gambar 2.4.

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 2.3 Flowchart Enkripsi



Gambar 2.4 Flowchart Dekripsi

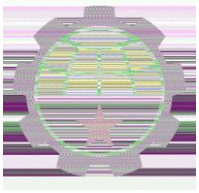
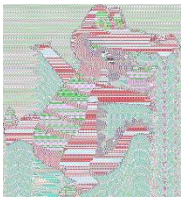
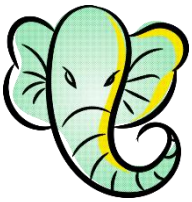
3. Hasil dan Pembahasan

Pada penelitian ini menggunakan beberapa gambar sebagai objek untuk di enkripsi. Gambar yang digunakan dibatasi dengan format png. Hasil enkripsi beserta kunci yang digunakan dapat dilihat pada tabel 3.1. Dimana ketika di dekripsi menggunakan kunci yang sama akan menghasilkan gambar asli yang di enkripsi.

Tabel 3.1 Hasil Enkripsi dan Dekripsi

Hasil Enkripsi	Kunci	Hasil Dekripsi
	harimau	
	anjing	

p-ISSN: 2986-3929
e-ISSN: 3032-1948

Hasil Enkripsi	Kunci	Hasil Dekripsi
	winniethepooh	
	earthstar	
	tyranosaurus	
	hapiness crocodile	
	elephanthead	

Pada penelitian ini dapat dilihat penggunaan Cipher Block Cipher dalam mengenkripsi pixel pada gambar masih belum maksimal. Dikarenakan secara kasat mata, hasil enkripsi masih berbentuk gambar aslinya, sehingga untuk mengamankan gambar tersebut masih kurang apabila menggunakan metode Cipher Block Chaining.

4. Kesimpulan

Pada penelitian ini dapat disimpulkan bahwa, penggunaan kriptografi dalam mengamankan sebuah gambar dengan cara mengenkripsinya sudah menghasilkan hasil yang cukup memuaskan. Penggunaan Cipher Block Chaining juga sudah menghasilkan gambar dengan warna yang berantakan. Gambarnya pun dapat dikembalikan ke gambar aslinya. Namun hasil enkripsi dengan metode ini masih kurang maksimal dikarenakan gambar hasil enkripsi masih memiliki pola yang sama dengan gambar aslinya. Ada baiknya apabila metode ini di kombinasikan dengan metode kriptografi modern lainnya untuk menghasilkan gambar enkripsi yang lebih abstrak. Sehingga tingkat keamanan gambar tersebut semakin tinggi.

Daftar Pustaka

[1] H. Sahara, “Implementasi Pengamanan Pesan Chatting menggunakan Metode Vigenere Cipher dan Cipher Block Chainning,” MEANS (Media Inf. Anal. dan Sist., vol. 3, no. 2, pp. 173–178, 2018.

[2] K. Informatika. “Perhitungan Manual Cipher Block Chaining Untuk Kriptografi Teks” available: http://www.kitainformatika.com/2019/05/perhitungan-manual-algoritma-chiper.html. (accessed Oct. 01 2021).

[3] D. Naufal, “Penjelasan Mengenai Cipher Block Chaining (CBC) dan Message Authentication Code (MAC), 29 November 2018.” available: https://medium.com/@dimas.naufal11/penjelasan-mengenai-cipher-block-chaining-cbc-dan-message-authentication-code-mac-39074d11f816. (accessed Oct. 01 2021).

p-ISSN: 2986-3929
e-ISSN: 3032-1948

Halaman ini sengaja dibiarkan kosong