Pengamanan Data Kombinasi Metode Cipher Block Chaining dan Modifikasi LSB

Data Security Combination of Cipher Block Chaining Method and LSB Modification

Wildan Mahmud[1], Ery Mintorini[2]
[1,2] STMIK Kadiri Kediri Jawa Timur Indonesia
E-mail: [1]wildan.mahmud@gmail.com, [2]ery_minto@yahoo.co.id

Abstrak

Perkembangan Internet dan aplikasi berbasis jaringan telah menjangkau ke berbagai macam aplikasi yang memungkinkan seseorang untuk saling berkirim pesan dan informasi tanpa dibatasi jarak dan waktu. Seiring dengan perkembangan itu pula, kerentanan akan aspek keamanan sebuah system juga semakin meningkat. Dalam penelitian ini, peneliti mencoba menerapkan kombinasi antara metode kriptografi dan steganografi yang bertujuan untuk meningkatkan upaya pengamanan sebuah pesan. Kriptografi Cipher Block Chaining (CBC) merupakan kriptografi yang sudah umum digunakan contohnya pada protocol internet TLS dan IPsec. Proses enkripsi dan dekripsi CBC memerlukan waktu yang relatif singkat karena mode CBC memiliki kecepatan dan efisiensi lebih tinggi dan dinilai lebih mudah diimplementasikan. Metode berikutnya yang digunakan adalah Steganografi Least Significant Bit (LSB) yang bekerja secara sederhana namun sangat efektif dalam menyisipkan pesan tersembunyi. Namun, beberapa penelitian menemukan kelemahan LSB yang dapat menemukan keberadaan pesan tersembunyi menggunakan algoritma *steganalytic* pada tingkat embedding yang rendah. Untuk itu, LSB harus dikembangkan lagi dengan menerapkan deteksi tepi sobel yang dapat bekerja untuk mendeteksi keypoint penyembunyian pesan sehingga LSB tidak lagi bekerja secara standar. Kombinasi metode CBC dan LSB-Sobel telah terbukti dan berhasil merahasiakan pesan dengan baik dan menghasilkan stego-image yang berkualitas tinggi setelah dilakukan pengujian PSNR dan MSE.

Kata kunci: Kriptografi, steganografi, CBC, LSB, Deteksi Tepi Sobel

Abstract

The development of the Internet and network-based applications has reached a variety of applications that allow one to send messages and information to one another without being limited by distance and time. Along with this development, the vulnerability of the security aspects of a system is also increasing. In this study, researchers tried to apply a combination of cryptographic and steganographic methods that aim to increase efforts to secure a message. Cryptography Cipher Block Chaining (CBC) is a cryptography that is commonly used for example in the TLS and IPsec internet protocols. The CBC encryption and decryption process requires a relatively short time because CBC mode has higher speed and efficiency and is considered easier to implement. The next method used is Least Significant Bit (LSB) Steganography that works simply but is very effective in inserting hidden messages. However, several studies have discovered the weakness of LSB that can find the presence of hidden messages using a steganalytic algorithm at a low embedding rate. For this reason, LSB must be developed further by implementing a single edge detection that can work to detect the hiding point of message hiding so that LSB no longer works by default. The combination of CBC and LSB-Sobel methods has been proven and successfully concealed messages well and produced high-quality stego-images after PSNR and MSE testing.

Keywords: Cryptography, steganography, CBC, LSB, Sobel Edge Detection

1. PENDAHULUAN

Teknologi informasi dan komunikasi saat ini telah membuat seseorang untuk saling bertukar pesan dan informasi tanpa dibatasi jarak dan waktu. Namun seiring dengan kemudahan yang ditawarkan, teknologi informasi juga semakin rentan terhadap serangan dan pencurian data dari pihak yang tidak bertanggung jawab. Beberapa solusi telah diusulkan dan diterapkan untuk melindungi pengguna teknologi dalam hal pengiriman pesan melalui jaringan komputer.

Kriptografi adalah salah satu metode pengamanan komputer yang dapat mengkonversi informasi atau pesan dari bentuk normal ke sebuah bentuk tak terbaca (terenkripsi) [1], [2]. Salah satu metode kriptografi yang termasuk dalam kriptografi modern dan memiliki kemampuan cukup handal adalah kriptografi Cipher Block Chaining (CBC) [2]–[4]. Proses enkripsi dan dekripsi CBC memerlukan waktu yang relatif singkat karena mode CBC memiliki kecepatan dan efisiensi lebih tinggi dan dinilai lebih mudah diimplementasikan. Operasi CBC merupakan algoritma kriptografi modern yang beroperasi pada level bit (0 atau 1) maupun sekelompok / blok bit dan bukan karakter. Penggunaan mode CBC menghasilkan ciphertext yang cukup rumit karena pada tiap blokknya saling bergantung satu sama lain sehingga sebuah kesalahan dalam satu blok saja akan mempengaruhi blok-blok berikutnya selama proses dekripsi data. Mekanisme mode CBC bekerja efektif untuk meningkatkan keamanan dalam menyediakan kerahasiaan data yang tinggi dan otentikasi[2], [4]–[6]. Operasi CBC memungkinkan untuk menerapkan mekanisme umpan balik pada sebuah blok bit dimana hasil dari proses enkripsi blok pertama digunakan sebagai *initialization vector* (IV) pada blok berikutnya dan dilakukan secara berulang sampai dengan blok bit yang tersedia habis. Hal ini menyebabkan setiap blok pada hasil enkripsi akan saling bergantung satu sama lain.

Selain kriptografi, metode lain yang biasa digunakan untuk menjaga keamanan dan kerahasiaan pesan adalah teknik steganografi. Steganografi merupakan seni dan ilmu yang dapat merahasiakan pesan dengan menyembunyikannya di dalam bidang lain. Terdapat berbagai metode yang digunakan dalam Teknik steganografi. Metode Least Significant Bit (LSB) dan Most Significant Bit (MSB) merupakan metode yang paling sering digunakan[7], [8]. Namun, LSB lebih sering digunakan karena LSB telah memenuhi syarat *fidelity, robustness* dan *recovery* serta lebih memiliki ketahanan terhadap gangguan *brightness* dan kontras. Konsep LSB yang cukup sederhana namun bekerja dengan sangat efektif dimana metode ini bekerja dengan menyisipkan pesan ke dalam bidang media (file gambar, video dsb) dengan cara memasukkan aliran bit rahasia ke dalam media tersebut. Namun, dari berbagai uji coba penelitian, keberadaan pesan tersembunyi LSB masih sangat mudah untuk dideteksi menggunakan algoritma *steganalytic* pada tingkat embedding yang rendah. Sehingga perlu peningkatan kemampuan agar pesan tersembunyi teserbut tidak mudah untuk ditemukan[9], [10].

Kelemahan pada metode LSB ini dapat dikurangi dengan menerapkan sebuah metode tambahan yaitu metode pendeteksian tepi. Pendeteksian tepi adalah metode yang paling umum digunakan untuk mendeteksi tepi pada greylevel. Metode deteksi tepi digunakan untuk mendeteksi *keypoint* penyisipan pesan sehingga LSB tidak lagi bekerja secara standar. Deteksi tepi dimanfaatkan untuk menyebarkan lokasi keypoint penyisipan pesan sehingga akan lebih sulit dideteksi oleh pihak yang tidak berkepentingan. Ada berbagai teknik deteksi tepi, salah satunya adalah deteksi tepi Sobel yang memiliki kemampuan mengurangi tingkat noise sebelum melakukan perhitungan pendeteksian tepi. Berdasarkan latar belakang tersebut, peneliti berusaha menerapkan model kombinasi kriptografi dan steganografi untuk dapat meningkatkan pengamanan pesan dan penyembunyian informasi yang mana akan dijelaskan secara detail pada bab selanjutnya.

2. METODE PENELITIAN

2.1 Pengumpulan Data

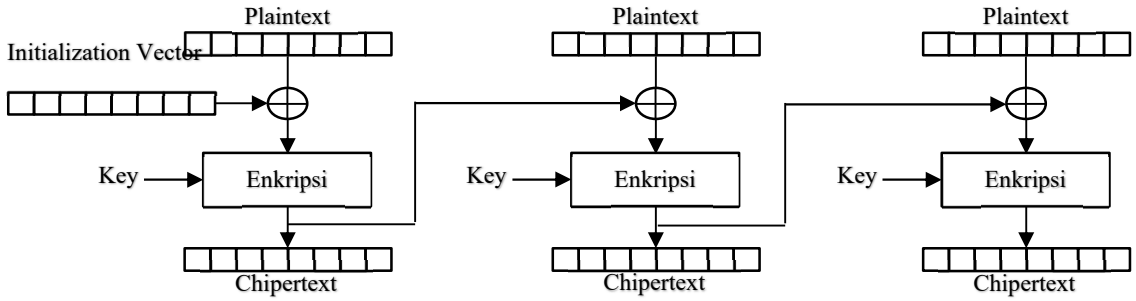
Dalam penelitian ini, diperlukan sebuah pesan (plaintext) yang ditujukan sebagai pesan rahasia yang akan dikirimkan. Pesan tersebut nantinya akan disimpan dalam format *.txt yang

akan dibuat secara random dengan jumlah 10 – 15 kata sebagai uji coba penelitian. Selain data text, diperlukan juga data citra 8-bit yang disimpan dalam format *.bmp yang nantinya akan digunakan sebagai citra cover dalam proses steganografi. Untuk pemilihan citra cover, jumlah keypoint pada citra cover haruslah lebih banyak daripada jumlah bit biner pada pesan sehingga semua bit biner pesan dapat disisipkan ke dalam citra cover[9]

2.2 Enkrispi menggunakan metode Cipher Block Chaining (CBC)

Pesan (plaintext) dalam bentuk teks dengan format .txt dienkripsi menggunakan algoritma Cipher Block Chaining (CBC) dengan merubah pesan ke dalam bentuk biner dan membagi biner pesan ke dalam blok-blok dengan ukuran 8 bit setiap bloknya[11]. Adapun proses enkripsi CBC adalah sebagai berikut.

a. Plaintext dibagi menjadi beberapa blok yang ditentukan ukurannya
b. Blok plain text pertama di-XOR-kan dengan IV (Initialization Vector)
c. Block hasil XOR dengan IV di-XOR-kan dengan kunci
d. Ciphertext hasil XOR dengan kunci ini kemudian menjadi IV pada blok berikutnya
e. Proses tersebut diulang kembali sampai blok terakhir.



Gambar 1 Mode Operasi CBC

2.3 Penerapan Deteksi Tepi Sobel

Deteksi tepi adalah pendekatan yang paling umum digunakan untuk mendeteksi diskontinuitas grey-level. Metode sobel menggunakan filter HPF (high pass filter) yang diberi satu angka nol penyangga dan merupakan pengembangan dari metode robert. Sobel memiliki kelebihan dalam kemampuannya untuk mengurangi noise sebelum melakukan perhitungan pendeteksian tepi. Operator Sobel melakukan pengukuran gradien spasial 2-D pada gambar dan menekankan daerah frekuensi spasial tinggi yang sesuai dengan tepi[10]. Dalam tahap ini, konvolusi masker dari Sobel detektor menunjukkan perbandingan dari pendeteksian tepi yang nantinya akan digunakan sebagai keypoint area penyimpanan pesan dalam proses steganografi.

2.4 Penyisipan Pesan menggunakan LSB

Teknik steganografi Least Significant Bit (LSB) bekerja dengan memanipulasi bit-bit terakhir pada byte-byte dalam suatu file gambar yang dijadikan sebagai media penyimpanan. Metode LSB standar memiliki kelemahan dimana metode ini tidak tahan terhadap statistical attack. Oleh karena itu, ditahap ini penggunaan metode pendeteksian tepi sobel diterapkan untuk membantu menyisipkan pesan yang sudah disandikan ke dalam cover-image menggunakan Teknik LSB yang mana telah ditentukan tepinya sebagai keypoint penyimpan pesan.

2.5 Pengujian Model Pengamanan Data

Tahap selanjutnya adalah mengukur tingkat keberhasilan atas metode yang diusulkan dalam menyisipkan pesan. Adapun Teknik pengujian yang diterapkan adalah penggunaan pengukuran MSE (Mean Square Error) dan PSNR (Peak Signal To Noise Ratio). Tujuan dari

pengujian ini adalah untuk mengetahui kualitas stego image yang sudah disisipkan pesan sandi, sudah berhasil berhasil disembunyikan atau tidak dengan melihat ukuran nilai MSE dan PNSR yang mana nilai dari MSE yang semakin rendah akan menghasilkan kualitas citra stego-image yang tidak berbeda dengan citra aslinya. Sedangkan PSNR yang semakin tinggi akan menghasilkan produk yang semakin baik[8], [12].

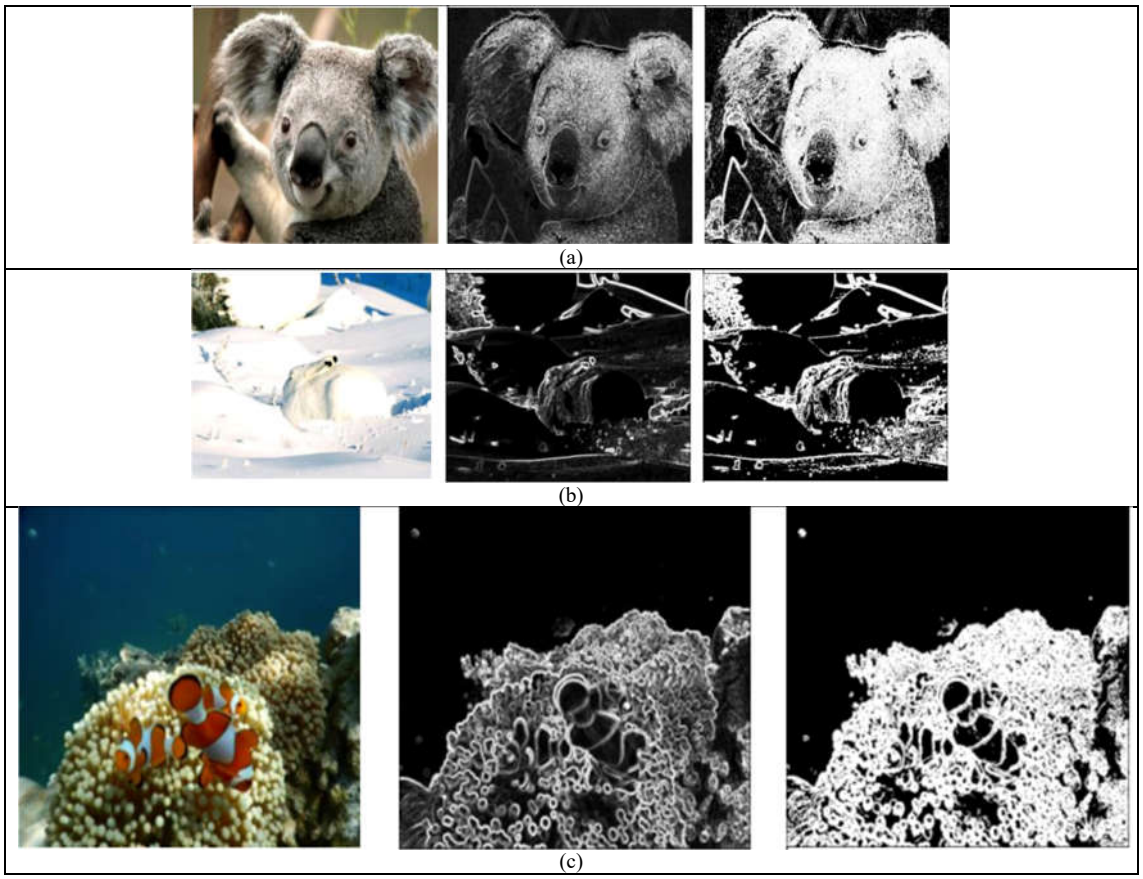
3. HASIL DAN PEMBAHASAN

Dalam penelitian ini, tahapan pertama yang dilakukan adalah mempersiapkan dataset yang akan digunakan. Peneliti menggunakan 3 buah file *.text yang berisikan pesan yang akan dikirimkan dan juga 3 buah file *.bmp yang digunakan sebagai media penyembunyian pesan yang akan dikirim. Untuk detailnya dapat dilihat pada Tabel 1 berikut.

Tabel 1 Rincian Dataset yang digunakan

Data Penelitian	
File citra Gbr1.bmp	
Pesan Jumlah dosen yang pembimbing, fasilitas perkuliahan dan kolaborasi antara mahasiswa dan dosen dalam membuat riset	
File citra Gbr2.bmp	
Pesan Makin banyaknya alumni yang diserap di dunia industri, serta bermanfaat bagi masyarakat luas	
File citra Gbr3.bmp	
Pesan Mendidik mahasiswa aktif, membekali alumni menghadapi dunia industri. Meningkatkan publikasi, penelitian, serta pengabdian pada masyarakat	

Proses selanjutnya adalah melakukan proses enkripsi CBC dengan nilai K= 01000010, IV = 01000010 yang kemudian akan menghasilkan ciphertext yang disimpan dalam cipher1.txt, cipher2.txt dan cipher3.txt. Setelah proses selesai, proses selanjutnya adalah mempersiapkan stego-image yang nantinya akan digunakan sebagai media penyisipan pesan. Citra yang sudah disiapkan yaitu Gbr1.bmp, Gbr2.bmp dan Gbr3.bmp diproses menggunakan algoritma deteksi tepi sobel agar mendapatkan koordinat keypoint yang digunakan untuk penyimpanan pesan. Adapun langkah pelaksanaannya adalah merubah citra menjadi grayscale; menjalankan algoritma sobel; menaikan threshold menjadi 40. Adapun hasil proses deteksi tepi sobel terlihat pada gambar 2.



Gambar 2 Proses Deteksi Tepi Sobel pada (a) Gbr1.bmp, (b) Gbr2.bmp, (c) Gbr3.bmp

Citra hasil deteksi tepi diberikan threshold sebesar 40 yang bertujuan untuk memperjelas tepi yang akan digunakan sebagai media penyimpanan. Diperoleh koordinat keypoint salah satu citra adalah sebanyak 105334 titik koordinat keypoint. Selanjutnya adalah proses penyisipan pesan terenkripsi kedalam media citra menggunakan metode LSB dengan memanfaatkan titik koordinat yang dihasilkan dengan metode deteksi sobel sebelumnya. Ujicoba proses penyisipan pesan cipher1.txt kedalam file citra Gbr1.bmp telah dilakukan dan menghasilkan file stego1.bmp yang telah berisikan pesan terenkripsi. Berikutnya adalah melakukan proses uji MSE dan PSNR untuk melihat perbedaan dari citra sebelum dan sesudah disisipkan pesan terenkripsi. Adapun hasil dari ketiga percobaan ditampilkan pada Tabel 2.

Tabel 2 Hasil Pengujian MSE dan PSNR

No	Keterangan	MSE	PSNR
1	Percobaan 1	0.0023	74.5058
2	Percobaan 2	0.0015	76.2783
3	Percobaan 3	0.0028	73.6396

Berdasarkan hasil pengujian non-attack pada tabel di atas, nilai MSE pada masing-masing stego-image cukup rendah dan nilai PSNR-nya cukup tinggi. Rata-rata nilai MSE pada citra uji adalah 0 dB dan rata-rata nilai PSNR-nya adalah di atas 70 pada citra hasil proses pengambilan pesan dengan citra pesan yang asli sehingga dapat dikatakan bahwa kualitas stegoimage yang dihasilkan dengan menggunakan metode yang diusulkan pada penelitian ini adalah baik.

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan oleh penulis, maka dapat disimpulkan beberapa hal bahwa model penggabungan teknik kriptografi CBC dan steganografi dengan metode LSB deteksi tepi Sobel dapat memperkuat keamanan dalam pengiriman pesan. Penelitian ini juga telah membuktikan bahwa pesan yang disisipkan ke dalam citra dapat diperoleh kembali secara utuh setelah diekstraksi tanpa mengalami kerusakan. Berdasarkan uji coba yang dilakukan, teknik penyisipan LSB dengan memanfaatkan deteksi tepi sobel menghasilkan kualitas citra yang cukup baik yaitu dengan rata-rata nilai MSE adalah 0 dB dan rata-rata nilai PSNR diatas 60. Maksud dari nilai MSE dan PSNR tersebut adalah bahwa citra hasil steganografi tidak berbeda jauh dengan citra asli sebelum steganografi sehingga akan sulit sekali dibedakan apakah citra tersebut ada pesan terenkripsi atau tidak.

DAFTAR PUSTAKA

[1] T. Yuniati, E. Suryani, and A. Aziz, "Pengaruh Variasi Panjang Kunci, Ukuran Blok, dan Mode Operasi Terhadap Waktu Eksekusi pada Algoritma Rijndael," *J. Teknol. Inf. ITSmart*, vol. 1, no. 1, p. 20, 2016.

[2] D. Rosmala and R. Aprian, "Implementasi Mode Operasi Cipher Block Chaining (CBC) Pada Pengamanan Data," *J. Inform.*, vol. 3, no. 2, pp. 55–66, 2012.

[3] A. P. Sidik *et al.*, "TEKNIK XOR PADA MODE OPERASI ALGORITMA CIPHER BLOCK CHAINING (CBC) DENGAN KUNCI ACAK BLUM BLUM SHUB DALAM MENINGKATKAN KEAMANAN DATA," *J. Mantik Penusa*, vol. 3, no. 2, pp. 130–135, 2019.

[4] E. K. Nurnawati, "Analisis Kriptografi Menggunakan Algoritma Vigenere Cipher Dengan Mode Operasi Cipher Block Chaining (CBC)," *Semin. Nas. Apl. Sains dan Teknol.*, no. IST AKPRIND Yogyakarta, pp. 266–272, 2008.

[5] N. Rochmah and Ardiansyah, "Desain Kriptografi CBC Modifikasi pada Proses Pengamanan Pesan melalui Email," *Semin. Nas. Teknol. Inf. dan Multimed.*, vol. 2, no. 1, pp. 1–6, 2016.

[6] C. B. Chaining, "Pengamanan Dokumen Teks Menggunakan Algoritma Kriptografi Mode Operasi Cipher Block Chaining (Cbc) Dan Steganografi Metode End of File (Eof)," *Techno.COM*, vol. 15, no. 1, pp. 22–31, 2016.

[7] Y. D. Setiyaningrum and A. Rohmani, "Penerapan Algoritma AES pada Dokumen Penting yang Disisipkan Dalam Citra Berbasis Algoritma LSB dan Sobel," *J. Inf. Syst.*, vol. 4, no. 2, pp. 178–189, 2019.

[8] M. Juneja and P. S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images," *Int. J. Comput. Commun. Eng.*, vol. 2, no. 4, pp. 513–517, 2013.

[9] D. R. I. M. Setiadi and J. Jumanto, "An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection," *Cybern. Inf. Technol.*, vol. 18, no. 2, pp. 74–88, 2018.

[10] A. M. Aaref, "Video Steganography Using LSB Substitution and Sobel Edge Detection," *Diyala J. Eng. Sci.*, vol. 11, no. 2, pp. 67–73, 2018.

[11] A. Muzakir, "Prototype Model Keamanan Data Menggunakan Kriptografi Data Encryption Standar (Des) Dengan Mode Operasi Chiper Block Chaining (Cbc)," *Semin. Nas. Inov. dan Tren 2014*, vol. 20, pp. 1–4, 2014.

[12] M. Wang, B. Cheng, and C. Yuen, "Joint Coding-Transmission Optimization for a Video Surveillance System with Multiple Cameras," *IEEE Trans. Multimed.*, vol. 20, no. 3, pp. 620–633, 2018.