Implementasi Kriptografi CBC dan Steganografi LSB Menggunakan Deteksi Tepi Sobel

ASTRID NUR AULIA
(Pembimbing : Adhitya Nugraha, S.Kom, M.CS)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201307852@mhs.dinus.ac.id

ABSTRAK

Internet dan aplikasi jaringan berkembang semakin cepat, memungkinkan seseorang untuk saling bertukar pesan, data atau informasi tanpa dibatasi oleh jarak dan waktu. Aspek keamanan dan pentingnya nilai dari data yang akan dipertukarkan melalui internet dan aplikasi jaringan juga seiring meningkat. Kriptografi merupakan kategori keamanan computer utama yang mengkonversi informasi dari bentuk normal ke dalam bentuk tak terbaca. Metode kriptografi yang cukup handal dan stabil dan menjadi induk dari algoritma kriptografi yang populer saat ini adalah Cipher Block Chaining (CBC) dan paling umum digunakan seperti pada protocol internet TLS dan IPsec. Selain kriptografi, untuk menjaga keamanan dan kerahasiaan pesan menggunakan teknik steganografi. Konsep LSB yang cukup sederhana sangat efektif untuk mengimplementasikan konsep steganografi. Namun LSB masih terbukti lemah, untuk itu digunakan metode pendeteksian tepi untuk memperbesar kapasitas penyisipan lebih banyak pada piksel tepi sehingga dapat menampung pesan lebih banyak tanpa terdeteksi. Penyembunyian pesan pada tepi citra adalah cara yang efisien untuk menyembunyikan pesan rahasia. Secara kasat mata akan sulit bagi manusia untuk membedakan perbedaan gambar sampul dengan stego-image yang pada tepinya telah disisipi pesan rahasia. Metode Sobel adalah pendeteksian tepi yang paling umum dan merupakan metode yang terbaik untuk mendeteksi tepi pada grey-level. Hasil penggabungan metode CBC dan LSB-Sobel ini dapat merahasiakan pesan dengan baik dan memiliki kualitas stego-image yang cukup tinggi setelah dilakukan pengujian menggunakan PSNR dan MSE.

Kata Kunci : Cipher Block Chaining, Least Significant Bit, Deteksi Tepi Sobel, PSNR & MSE

Implementation of CBC Cryptography and Steganography LSB Using Sobel Edge Detection

ASTRID NUR AULIA
(Lecturer : Adhitya Nugraha, S.Kom, M.CS)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201307852@mhs.dinus.ac.id

ABSTRACT

Internet and network applications grow more quickly, allowing them to exchange messages, data or information without being limited by time and distance. The security aspect and the importance of the value of the data to be exchanged over the Internet and network application are more increasing. Cryptography is the main category of computer security that converts information from the normal form into a form unreadable. Cryptographic methods are quite reliable and steady and became the main of a cryptographic algorithm that is popular today is the Cipher Block Chaining (CBC) and the most commonly used in Internet protocols such as TLS and IPsec. In addition to encryption, to safeguard the security and confidentiality of the message can using steganographic techniques. Fairly simple concept of LSB is very effective to implement the concept of steganography. However LSB proven still weak, therefore edge detection method is used to enlarge the capacity of insertion more on edge pixels so it can accommodate more messages without being detected. Concealment message on the edge of the image is an efficient way to hide secret messages. In plain would be difficult for a human to distinguish the difference image with the stego-image cover that the edges have inserted a secret message. Sobel edge detection method is the most common and is the best method to detect the edges of the gray-level. The result of the incorporation of methods LSB-Sobel and CBC can keep the message very well and had a quite high stego-image quality after testing using PSNR and MSE.

Keyword : Cipher Block Chaining, Least Significant Bit, Sobel Edge Detection, PSNR and MSE