VIGENERE CIPHER PADA PENYISIPAN PESAN LSB-SIFT

Fatkhurul Dewi Khotimah [1], Guruh Fajar Shidik[2]
[1,2]UDINUS
Jl Nakula 1 No. 5-11, Semarang, 50131, (024)3517261
E-mail : 111201105884@mhs.dinus.ac.id[1], guruh.shidik@dsn.dinus.ac.id[2]

Abstrak

Teknologi informasi merupakan gabungan antara teknologi komputer dan teknologi telekomunikasi yang membentuk sistem dan bekerjasama untuk melakukan pengolahan, pengumpulan, penyimpanan sampai pengiriman informasi. Keamanan teknologi menjadi pusat perhatian, kejahatan di dunia maya pun semakin meningkat. Istilah yang sering disebut yaitu cyber crime, identik dengan kejahatan yang mengambil atau memodifikasi suatu informasi yang bukan haknya. Oleh karena itu muncul teknik pengamanan data yaitu dengan kriptografi dan steganografi. Algoritma Vigenère Cipher merupakan algoritma kriptografi yang biasa digunakan untuk penyandian. Sedangkan Least Significant Bit (LSB) untuk menyisipkan data ke bit terakhir dari setiap piksel pada cover image. Kelemahan pada kedua algoritma ini membuat peneliti termotivasi untuk memodifikasi algoritma LSB dengan metode SIFT. Scale Invariant Feature Transform(SIFT) digunakan untuk menetukan kemiripan dua citra. Cover-object akan dilakukan proses SIFT dengan input citra pembanding. Keypoint akan disisipkan pesan hasil enkripsi menggunakan algoritma LSB. Selanjutnya dilakukan evaluasi dengan menghitung MSE dan PSNR pada citra yang dilakukan attack maupun non attack.

Kata Kunci: *Kriptografi, Steganografi, Vigenere Cipher, Hill Cipher, Penyembunyian Informasi, LSB, SIFT.*

Abstract

Information technology is combination between computer technology and communication technology that form system and cooperate to process, collect, store and transfer information. Security technology become attention, crime in cyberspace also increased. Most common term is cybercrime, identic with crime that take or modify information that is not his or her copyright. That's why security technique created, it is called cryptography and steganography. Vigenère Cipher Algorithm is cryptography algorithm that usually used to encrypt a message. While Least Significant Bit (LSB) for inserting data to last bit from every pixel on cover image. Weakness from this two algorithm cause researcher motivated to modify LSB to SIFT method. Scale Invariant Feature Transform (SIFT) is to determine similarity between two image. Cover-object will processed with SIFT with image for comparison. Keypoint will be inserted by encrypted message using LSB algorithm. Furthermore will be evaluated with counting MSE and PSNR on attacked or not attacked image.

Keywords: *Cryptography, Steganography, Vigenere Cipher, Hill Cipher, Information Hiding, LSB, SIFT.*

1. PENDAHULUAN

Di abad modern ini, teknologi informasi berkembang sesuai dengan perannya dalam membantu pekerjaan manusia. Teknologi informasi merupakan seperangkat alat yang membantu pekerjaan yang berkaitan dengan informasi dan melakukan tugas-tugas yang berhubungan dengan pemrosesan informasi serta mendistribusikan informasi tersebut dengan menggunakan saluran komunikasi. Teknologi informasi merupakan gabungan antara teknologi komputer dan teknologi telekomunikasi yang membentuk suatu sistem dan bekerja bersama-sama untuk melakukan pengolahan informasi pengumpulan, pengolahan, penyimpanan sampai

pendistribusian (pengiriman) informasi [1]. Citra (image) merupakan gambar pada bidang dua dimensi yang dihasilkan dari gambar analog dua dimensi dan kontinus menjadi gambar diskrit, melalui proses sampling gambar analog dibagi menjadi M baris dan N kolom sehingga menjadi gambar diskrit [2].

Dalam dunia sekarang ini keamanan teknologi menjadi pusat perhatian. Dengan meningkatnya kejahatan di dunia maya (cyber crime), menyediakan keamanan jaringan saja tidak cukup. Keamanan yang disediakan gambar seperti blue print dari perusahaan, gambar rahasia yang digunakan dalam militer atau kepentingan perusahaan [3]. Karena hal tersebut munculah teknik pengamanan pesan yaitu kriptografi dan steganografi. Kriptografi diciptakan sebagai suatu teknik untuk mengamankan kerahasiaan komunikasi. Berbagai metode telah dikembangkan untuk mengenkripsi dan mendekripsi data untuk menjaga kerahasiaan pesan. Teknik kriptografi saja tidak cukup untuk menjaga kerahasiaan pesan, sehingga diperlukan teknik steganografi untuk menyembunyikan pesan dengan suatu cara sehingga tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia yang disisipkan [4].

Algoritma Vigenère Cipher dan Hill Cipher merupakan algoritma kriptografi yang biasa digunakan untuk penyandian atau kriptografi. Konsep dari algoritma ini adalah sebuah data akan disandikan berdasarkan metode tertentu sehingga orang yang berkepentingan dan tidak memiliki hak akses akan mengalami kesulitan untuk melakukan hal-hal yang tidak diinginkan. Sebaliknya ketika data tersebut akan diakses kembali oleh orang yang berhak maka hasil penyandian tersebut akan dikembalikan ke bentuk semula. Alasan pemilihan algoritma Vigenère Cipher karena Vigenère Cipher mengubah pesan dengan menggunakan kombinasi 26 huruf alfabet dan algoritma ini bertahan cukup lama sampai ditemukannya metode untuk memecahkan algoritma tersebut [5]. Hill Cipher mengubah pesan dengan melakukan perkalian matrix dan operasi modulo untuk membandingkan kecepatan dan hasil enkripsi pada citra.

Penelitian Angelina [6] menggunakan algoritma Vigenère Cipher untuk melakukan enkripsi pada citra. Metode yang digunakan pada pemrosesan dengan menggunakan metode Vigenère pada komputer antara lain tabel konversi dan operasi nilai ASCII, tetapi tidak bisa diterapkan pada image, diperlukan suatu adaptasi agar algoritma semacam itu bisa bekerja pada image. Algoritma modifikasi dari Vigenère Cipher ini sangat sederhana, walaupun tidak diketahui seberapa efektivitasnya.

Penelitian Basuki Rakhman [7] menggunakan metode Least Significant Bit dengan kombinasi Algoritma Kriptografi Vigenère dan RC4 untuk memberikan proteksi ganda pada pesan rahasia di dalam sebuah gambar.

Dalam steganografi banyak metode yang dikembangakan, salah satu metode yang umum digunakan adalah metode Least Significant Bit (LSB). LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan [7]. Tujuan dari metode LSB yaitu mampu menyembunyikan informasi yang berukuran minimal dan hanya mampu menyimpan informasi dengan ukuran sangat terbatas, hal ini mendorong dikembangkannya suatu tambahan untuk meningkatkan kemampuan suatu aplikasi steganografi yang menggunakan metode modifikasi Least Significant Bit (LSB). Metode LSB ini tidak mengubah kualitas citra yang signifikan dengan persepsi manusia karena hanya mengubah pada bit terakhir citra [8].Menurut penulis steganografi akan lebih baik jika

digunakan pada citra grayscale karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia [9]. Citra grayscale yang hanya mempunyai 8 bit saja ternyata mampu mengolah citra dengan lebih cepat daripada citra RGB [10].

Untuk mengatasi kelemahan algortima LSB, maka pada penelitian ini dilakukan penggabungan dengan algoritma Scale Invariant Feature Transform (SIFT). SIFT merupakan algoritma yang dapat diaplikasikan pada image matching yang memiliki ketahanan terhadap citra yang mengalami perubahan transformasi seperti rotasi, ditemukan oleh David G. Lowe pada tahun 1999, seorang peneliti dari University of British Columbia. Dalam penelitian ini algoritma SIFT suatu citra akan di ubah menjadi vektor fitur lokal yang kemudian akan digunakan sebagai pendekatan dalam mendeteksi objek yang dimaksud. Secara garis besar, algoritma yang digunakan pada metode SIFT terdiri dari empat tahap, yaitu mencari nilai ekstrim pada skala ruang, menentukan keypoint, penentuan orientasi, dan deskriptor keypoint [11].

Scale Invariant feature transform merupakan salah satu algoritma yang bekerja cukup baik dalam mendeteksi ciri pada suatu citra, output dari algoritma ini berupa titik titik kunci yang berada di sekitar pola dari citra yang biasa disebut dengan keypoint descriptor yang mana nantinya keypoint descriptor dari sebuah citra dapat dibandingkan dengan keypoint descriptor pada citra lain yang selanjutnya dapat ditentukan tingkat kemiripannya [11]. Titik-titik kunci inilah yang akan digunakan untuk menyisipkan pesan yang telah dienkripsi menggunakan algoritma LSB.

Berdasarkan penelitian dari jurnal Basuki Rakhmat dan Mauhammad Fairuzabadi [7] algoritma Vigenère Cipher dapat digabungkan dengan teknik steganografi. Berdasarkan penelitian tersebut, penulis mengembangkan aplikasi kriptografi perlu mengkombinasikan dua algoritma untuk mendapatkan proteksi ganda yang lebih baik dalam menjaga keamanan dan kerahasiaan pesan, serta terintegrasi dengan steganografi untuk menyembunyikan pesan dalam sebuah gambar bitmap guna melindungi keberadaaan pesan rahasia. Pada jurnal [12] menyatakan bahwa teknik kriptografi dapat digabungkan dengan teknik steganografi dengan modifikasi menggunakan algoritma SIFT untuk dijadikan key dan hasilnya sangat aman untuk transaksi data dalam waktu dekat. Oleh karena itu, penulis memiliki ide untuk menggabungkan teknik kriptografi, yaitu dengan algoritma Vigenère Cipher, dan teknik steganografi yaitu dengan algoritma LSB. Algoritma LSB akan dimodifikasi dengan algoritma Scale Invariant Feature Transform (SIFT). Penggunaan algoritma Vigenère Cipher, LSB, dan SIFT diharapkan dapat meningkatkan keamanan pesan dan mengatasi kelemahan dari algoritma Vigenère Cipher dan LSB..

2. METODE

Dalam penelitian ini yang terdiri dari dua proses utama, yaitu proses untuk merahasiakan pesan dan proses untuk pengambilan pesan.

2.1 Penyisipan pesan

Untuk melakukan penyisipan pesan, terlebih dahulu pesan di enkripsi, kemudian membuat map penyisipan dan melakukan penyisipan tiap bit pesan pada LSB cover.

2.1.1 Enkripsi pesan

1. Input pesan gambar (plain image) dan

k sebagai kunci Vigenère Cipher.
2. Lakukan penjumlahan tiap pixel ke n dengan kunci ke n, apabila dalam melakukan penjumlahan panjang kunci lebih dari jumlah pixel maka kunci Vigenère Cipher, maka kunci diulang dari awal.
3. Hitung modulo 256 dari hasil penjumlahan plain image dan key.
4. Output pada tahap enkripsi pesan ini adalah file citra yang sudah diacak bentuknya (disebut sebagai cipher image).

2.1.2 Map penyisipan

1. Input cover-object dan citra pembanding.
2. Menentukan scale-space extrema detection.
3. Menentukan keypoint localization.
4. Menetukan orientation assignment.
5. Menentukan keypoint descriptor.
6. Hasil pada tahap ini berupa keypoint untuk map penyisipan.

2.1.3 LSB

1. Input cipher image, cover, dan map penyisipan.
2. Mengubah nilai piksel citra cipher image bilangan biner.
3. Masukan tiap bit cipher image ke LSB dari map penyisipan cover.
4. Output pada tahap penyisipan pesan ini berupa file stego-image.

2.2 Pengambilan pesan

Untuk melakukan pengambilan pesan, terlebih dahulu membuat map ekstraksi, kemudian mengambil tiap bit pesan pada LSB citra stegano di lokasi map ekstraksi dan melakukan dekripsi pada citra hasil ekstraksi.

2.2.1 Map Ekstraksi

1. Input stego-image dan citra pembanding.
2. Menentukan scale-space extrema detection.
3. Menentukan keypoint localization.
4. Menetukan orientation assignment.
5. Menentukan keypoint descriptor.

2.2.2 Ekstraksi pesan

1. Input file stego-image dan map ekstraksi.
2. Mengubah nilai piksel stego-image menjadi bilangan biner.
3. Melakukan pengambilan bit LSB stego-image. Posisi pengambilan dilakukan berurutan sesuai dengan urutan posisi angka dalam map ekstraksi. Misalkan keypoint yang pertama pada angka 1 berada di pojok kiri atas, yang berarti posisi (0,0) dalam citra digital, maka bit biner ke-1 dari ciphertext disisipkan pada piksel cover di posisi (0,0). Kemudian keypoint yang kedua terletak pada angka 4 berada di sebelah kanan angka 1, yang berarti posisi (0,4) dalam citra digital, maka bit biner ke-2 dari ciphertext disisipkan pada piksel cover di posisi (0,4). Begitu seterusnya hingga mencapai angka (m * n * 8). Pengambilan bit LSB hanya sampai (m * n * 8) agar dapat sesuai dengan jumlah bilangan biner pada ciphertext.
4. Menyiapkan sebuah persegi berukuran m x n sebagai tempat untuk menyusun kembali ciphertext.
5. Mengubah kembali barisan bilangan biner yang telah diambil pada langkah ke-3 menjadi angka yang merepresentasikan nilai derajat keabuan piksel. Setiap 8-bit biner berarti 1 warna. Misalkan terdapat barisan 1111111100000000, berarti dipisah menjadi 11111111 00000000, yang berarti 255 0.
6. Memasukkan nilai derajat keabuan pada tahap ke-5 dalam persegi yang telah dibuat pada tahap ke-4 secara berurutan (dari kiri ke kanan).
7. Output pada tahap ini adalah cipherimage.

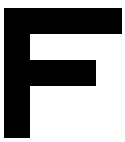
2.2.3 Dekripsi pesan

1. Input file cipherimage dan kunci Vigenère Cipher.
2. Lakukan dekripsi pada pixel gambar dengan rumus dekripsi Vigenère.
3. Output pada tahap ini adalah gambar pesan asli.

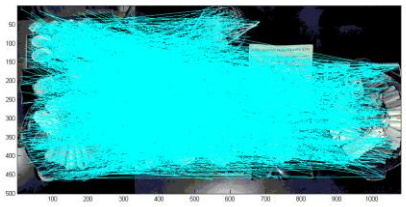
2.3 Tabel dan Gambar

Gambar 1. Citra Cover

Gambar 2. Citra Pembanding



Gambar 3. Citra pesan (12 x 12 pixel)



Gambar 4. Match cover dan pembanding

Tabel 1: Tabel MSE PSNR

Citra yang dibandingkan		MSE	PSNR
Cover	Stegano	0.0016	76.1954
Pesan Asli	Pesan Stegano	0	inf
Cover	Stegano salt&pepper	256.54	24.03
Cover	Stegano scratch	134.71	26.83
Pesan Asli	Pesan Stegano salt&pepper	675.5	19.69
Pesan Asli	Pesan Stegano Scratch	0	Inf

3. Hasil Eksperimen

Citra hasil ekstraksi dapat diambil kembali, namun untuk penyerangan dengan salt & pepper, pesan mengalami perubahan.

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan oleh penulis, maka dapat disimpulkan beberapa hal sebagai berikut:

1. Penggabungan teknik kriptografi dan steganografi yaitu dengan melakukan enkripsi pesan menggunakan metode Tradisional Cipher, kemudian menyisipkannya kedalam Cover dengan metode LSB yang posisinya ditentukan oleh keypoint hasil SIFT.
2. Setelah dilakukan penyerangan dengan scratch dan salt & pepper kualitas stego-image menurun drastis, dilihat dari MSE yang tinggi mencapai lebih dari 130 dan PSNR yang rendah mencapai 24 desibel. Sedangkan untuk pesan yang di ekstrak mengalami perubahan MSE mencapai lebih dari 500 dan PSNR kurang dari 20 desibel.
3. Vigenere Cipher lebih unggul dari Hill Cipher dalam kecepatan enkripsi dan dekripsi pesan.

DAFTAR PUSTAKA

[1] N. D. Nathasia and A. E. Wicaksono, "Penerapan Teknik Kriptografi Stream-Cipher Untuk Pengaman Basis Data," ICT Research Center UNAS, vol. 6, no. 1. pp. 1–22, 2011.

[2] M. R. Kumaseh, L. Latumakulita, N. Nainggolan, and S. Citra, "Segmentasi Citra Digital Ikan Menggunakan Digital Fish Image Segmentation By Thresholding Method."

[3] T. Joutou and K. Yanai, "A food image recognition system with Multiple Kernel Learning," Image Process. (ICIP), 2009 16th IEEE Int. Conf., vol. 5, no. 2, pp. 13–21, 2009.

[4] L. S. Bit, M. Jurusan, and T. Elektro, "MAKALAH SEMINAR TUGAS AKHIR DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA JPEG Jurusan Teknik Elektro Fakultas Teknik Universitas Diponegoro kedalam pesan lainnya yaitu file citra dengan menggunakan algoritma LSB (Least Significant Bit) pada suatu aplikasi."

[5] E. K. Nurnawati, "Analisis Kriptografi Menggunakan Algoritma Vigenere Cipher Dengan Mode Operasi Cipher Block Chaining (Cbc)," pp. 266–272, 2008.

[6] L. Angelina, I. T. Bandung, and J. G. Bandung, "Penerapan dari Pengembangan Algoritma Vigenere dalam Enkripsi Image," no. 13506117, pp. 1–6, 2011.

[7] Basuki Rakhmat; Muhammad Fairuzabadi, "Steganografi Menggunakan Metode Least Significant Bit Dengan Kombinasi Algoritma Kriptografi Vigenère Dan Rc4," Zhurnal Eksp. i Teor. Fiz., vol. 5, no. September, pp. 1–17, 1937.

[8] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB steganography and its evaluation for various bits," 2006 1st Int. Conf. Digit. Inf. Manag. ICDIM, vol. 872, pp. 173–178, 2006.

[9] A. Ilmiah, "Perancangan dan Implementasi Aplikasi Steganografi pada Citra Menggunakan Metode LSB Termodifikasi dalam Pemilihan Byte Penyisipan Perancangan dan Implementasi Aplikasi Steganografi pada Citra Menggunakan Metode LSB Termodifikasi dalam Pemilihan Byte Peny," no. 672008107, 2013.

[10] D. E. Walia, P. Jain, and N. Deep, "An Analysis of LSB & DCT Based Steganography," Glob. J. Comput. Sci. Technol., vol. 10, no. 1, pp. 4–8, 2010.

[11] S. Jatmiko, "Analisis Dan Implementasi Penggunaan Scale Invariant Feature Transform (SIFT) Pada Sistem Verifikasi Tanda Tangan," 2013.

[12] A. Gangwar, "Improved RGB - LSB Steganography Using Secret," vol. 4, pp. 85–89, 2013.

[13] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-qershi, "A Comparison between Using SIFT and SURF for Characteristic Region Based Image Steganography," vol. 9, no. 3, pp. 110–116, 2012.

[14] I. Kriptografi and D. A. N. Steganografi, "Pada Media Gambar Dengan Menggunakan Metode Des Dan Region-Embed Data Density .," Byte, pp. 1–7, 2011.

[15] K. J. Devi, "A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding

Technique by," no. May, 2013.

[16] D. K. Budiarsyah, "Pengujian Beberapa Teknik Proteksi Watermark Terhadap Penyerangan," 2013.