KOMBINASI STEGANOGRAFI BIT MATCHING DAN KRIPTOGRAFI PLAYFAIR CIPHER, HILL CIPHER DAN BLOWFISH

Budi Wijaya Rauf

Magister Teknik Informatika, Universitas Amikom Yogyakarta
Jl. Ring Road Utara, Ngringin, Condong Catur, Depok, Sleman, Yogyakarta
budi0029@students.amikom.ac.id

Abstract *- To secure data, cryptographic techniques are needed, but many cryptographic methods are vulnerable that require attacks. But not with the Blowfish method which includes a symmetric key algorithm that has the same key to encrypt and decrypt data. The blowfish algorithm is a block cipher and until now. Blowfish is still superior in the field of strength endurance will receive attacks from outside by people who are not responsible. In this study, a test will be carried out to see the time used to make a suitable steganographic combination and to combine several cryptographic methods such as Playfair, hill cipher, and blowfish. The average embedding average 28.275 seconds embedding extraction 27.843 seconds and for imaging the average embedding 13.0208 seconds and extraction 12.7986 seconds.*
Keywords *- Steganography, Playfair, Hill Cipher, Blowfish. Bit Matching*

Abstrak **-** Untuk melakukan pengamanan data dibutuhkan tekhnik kriptografi akan tetapi sudah banyak metode-metode kriptografi yang rentan terkena serangan. Namun tidak dengan metode Blowfish yang termasuk algoritma kunci simetris yang memiliki kunci yang sama untuk mengenkripsi dan mendekripsi suatu data. Algoritma Blowfish merupakan cipher blok dan sampai saat ini algoritma Blowfish masih unggul dibidang ketahanannya yang kuat akan menerima serangan dari luar oleh orang-orang yang tidak bertanggung jawab. Pada penelitian kali ini akan dilakukan pengujian untuk melihat waktu yang dipakai untuk melakukan kombinasi steganografi bit matching serta mengkombinasikan beberapa metode kriptografi seperti playfair, hill cipher dan blowfish. Hasilnya ialah untuk citra hitam putih diperoleh waktu rata-rata *embedding* 28.275 detik ekstraksi 27.843 detik dan untuk citra berwarna waktu rata-rata embedding 13.0208 detik dan ekstraksi 12,7986 detik.
Kata Kunci - Steganografi, Playfair, Hill Cipher, Blowfish, Bit Matching.

I. PENDAHULUAN

Dengan berkembangnya zaman, maka kebutuhan manusia pun semakin meningkat.Perkembangan ini didasari oleh internet yang telah dikembangkan, namun dalam menjelajahi dunia maya, kita harus berhati-hati karena banyaknya penyalahgunaan data dan penyebaran informasi sensitive yang menyalahi norma-norma yang ada dalam masyarakat. Berbagai mesin pencari telah berkembang yang dulu hanya sekadar mencari kini memiliki fitur pemindai virus, anti spam dan mekanisme keamanan lainnya. Hal ini dilakukan guna meningkatkan keamanan data/informasi pribadi individu, salah satu ilmu yang saat ini digunakan untuk mengamankan data adalah kriptografi dan steganografi.

Steganografi merupakan seni dan ilmu menyembunyikan data kedalam media lain sebagai penutup (cover) salah satunya citra/gambar[1]. Kriptografi adalah seni dan ilmu untuk menjaga kerahasiaan data, data tersebut diubah atau bahasa ilmiahnya di enkripsi sehingga tidak dapat dibaca oleh orang lain[2]. Dengan menggabungkan dua metode tersebut, maka dapat meningkatkan keamanan data. Penggabungan metode steganografi dan kriptografi telah banyak dikembangkan dalam kurun waktu 10 tahun ini, pada umumnya teknik ini digunakana dengan mengenkripsi pesan terlebih dahulu, kemudian menyisipkan pesan tersebut ke media cover. Tetapi, proses tersebut beresiko mengubah kualitas pada cover(citra). Untuk meminimalisir resiko tersebut maka dilakukan penyisipan pada bit terakhir. Perubahan kualitas cover tidak akan terlalu nampak secara kasat mata.

Penelitian dilakukan oleh Prasetyo, dkk (2019), yang melakukan kombinasi steganografi bit matching dengan kriptografi DES untuk memperkuat keamanan data. Kelebihan dari penggabungan dua metode tersebut ialah citra tidak mengalami perubahan bahkan kapasitas pesan yang dapat ditampung dapat lebih besar dari sebelumnya. Hasil pengujian menunjukkan citra hitam putih maupun berwarna dapat digunakan sebagai cover, terkecuali citra dengan warna 100% hitam atau 100% putih. Pencocokan dengan citra yang berwarna terkesan lebih cepat. Kerusakan pesan dengan penambahan noise salt dan peper mulai terjadi pada nilai MSE 0.00067 dan gaussian mulai terjadi pada MSE 0.000234[3].

Penelitian yang dilakukan Suhandinata dkk (2019) menganalisa performa dari metode hybrid dan Blowfish serta RSA. Hasilnya adalah metode hybrid memiliki performa tidak jauh berbeda daripada blowfish bahkan membuat enkripsi dan dekripsi data

lebih aman. Rata-rata kecepatan enkripsi algoritma hybrid untuk dokumen 0,85 detik, gambar 1,06 detik, audio 3,38 detik, dan video 15,56 detik. Sedangkan rata-rata kecepatan dekripsi algoritma hybrid untuk dokumen 1,01 detik, gambar 1,38 detik, audio 4,3 detik, dan video 27,56 detik[4].

Penelitian berikutnya yang dilakukan Wowor (2013), dengan memodifikasi metode Hill Cipher dengan Convert Between Base. Dengan adanya modifikasi ini dapat mempersulit kriptanalis dalam menganalisa hasil cipher teks karena memiliki bit elemen dengan perkalian matriks yang memiliki fungsi linier[5].

Kurniawan (2017), melakukan pengimplementasian kriptografi dengan algoritma RSA dengan Playfair Cipher. Hasilnya adalah algoritma RSA dapat diperkuat dengan dimodifikasi kuncinya dienkripsi terlebih dahulu dengan playfair lalu baru setelah itu didekripsi[6].

Berdasarkan latar belakang masalah tersebut, peneliti ingin menghasilkan keamanan data yang lebih ketat lagi dengan mengkombinasikan algoritma steganografi bit matching dengan beberapa algoritma kriptografi seperti playfair cipher, hill cipher dan blowfish.

A. *Kriptografi*

Algoritma kriptografi berasal dari bahasa Yunani, yaitu crypto yang berarti rahasia dan graphia yang berarti tulisan. Kriptografi merupakan seni dan ilmu dalam menjaga keamanan pesan yang akan dikirim ke satu tempat ke tempat yang lain. Algoritma kriptografi merupakan adalah urutan langkah-langkah logis untuk merasahasiakan informasi dari orang-orang yang tidak berhak. Menurut Amita Pandey, dasar konsep kriptografi terdiri dari [7]:

a. Plain text, adalah pesan asli yang ingin dikirim.
b. Cipher text, adalah pesan yang tidak dapat dimengerti oleh siapapun yang awalny amerupakan plain text.
c. Encryption,mengkonversi plain text menjadi cipher text, membutuhkan 2 proses, algoritma enkripsi dan kunci.
d. Decryption, mengkonversi cipher text menjadi plain text, membutuhkan 2 proses, algoritma dekripsi dan kunci.
e. Key, merupakan kombinasi dari angka atau huruf atau symbol spesial yang digunakan dalam enkripsi dan dekripsi dan memiliki peran penting dalam kriptografi karena algoritma bergantung kepadanya. Algoritma kriptografi dapat diklasifikasikan menjadi 3 berdasarkan jenis kuncinya, kriptografi kunci simetris, kriptografi kunci asimetris dan kriptografi hybrid.

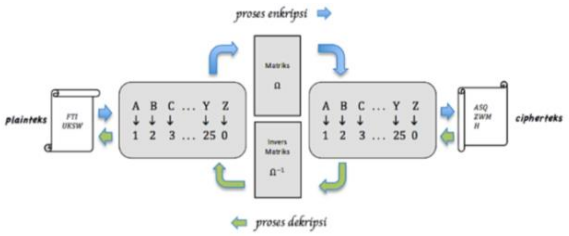
B. *Playfair Cipher*

Playfair Cipher ditemukan oleh sir Charley Wheatstone pada tahun 1854 lalu dipopulerkan oleh Baron Lyon Playfair, yang namanya lalu diabadikan menjadi nama algoritma. Meskipun algoritma playfair ini sudah tidak lagi aman untuk digunakan, namun algoritma ini masih sangat efektif. Playfair cipher pertama kali digunakan oleh seorang berkebangsawan inggris pada perang Boer dan perang dunia I. Playfair ini merupakan salah satu algoritma klasik yang masuk ke dalam polygram cipher, dalam plainteks diubah menjadi bentuk poligram dan proses enkripsi dan dekripsi dilakukan untuk poligram. Kuncinya adalah 25 huruf yang disusun ke dalam sebuah bujur sangkar berdimensi 5x5 dengan menghilangkan salah satu hurufnya (j). Kemungkinan kuncinya ialah 25!. Susunan yang ada pada bujur sangkar lalu diperluas dengan menambahkan kolom keenam dan baris keenam. Baris keenam merupakan baris pertama sementara kolom keenam merupakan kolom pertama. Biasanya, kunci yang digunakan adalah yang mudah untuk dimengerti. Pesan yang telah dienkripsi lalu akan diatur terlebih dahulu dengan aturan sebagai berikut [8] :

a. Ganti huruf J dengan I
b. Tulis huruf dari pesan tersebut secara berpasangan.
c. Ketika ada huruf pesan yang sama maka sisipkan Z di tengahnya.
d. Jika jumlah huruf ganjil maka tambahkan Z diakhir pasangan huruf tersebut.

C. *Hill Cipher*

Proses enkripsi-dekripsi Hill cipher secara umum dapat digambarkan



Gambar 1. Proses Enkripsi-Dekripsi Hill cipher

Matriks bujursangkar Ω berordo $n \times n$ yang mempunyai invers untuk dijadikan kunci. Misalkan P sebagai plainteks yaitu dan C sebagai cipherteks sehingga proses enkripsi adalah [9]

$$C = \Omega \cdot P \ (mod\ 26) \quad (1)$$

Proses dekripsi secara umum diberikan $P = \Omega{-}1 \cdot C$ $(mod\ 26)$ (2)

D. *Blowfish*

Blowfish atau biasa disebut dengan "OpenPGP.Cipher.4" merupakan algoritma kunci yang simetris dengan cipher blok dan dirancang pada tahun 1993 oleh Bruce Schneider untuk menggantikan DES (Data Encryption Standard). Algoritma ini dibuat untuk digunakan pada komputer yang memiliki microprosesor yang besar (32 bit keatas).

Pada saat itu, banyak algoritma yang patennya dimiliki secara khusus oleh Amerika Serikat, sehingga tidak dapat digunakan oleh orang lain. Namun, Schneider mengatakan bahwa blowfish ini akan selalu berada pada domain publik sehingga bisa digunakan oleh banyak pihak. Dengan pernyataannya tersebut, Schneider mendapat banyak perhatian dan memiliki tempat khusus di dunia kriptografi.

Blowfish memiliki kriteria sebagai berikut [10] :

a. Cepat, Blowfish memiliki kecepatan dengan rate 26 clock per byte saat melakukan enkripsi data dengan microprosesor 32-bit.

b. Compact, Blowfish tetap dapat berjalan dengan hanya menggunakan memory 5.000 byte.

c. Sederhana, Blowfish menggunakan operasi yang sangat sederhana seperti : penambahan, XOR, dan lookup pada tabel operan 32 bit.

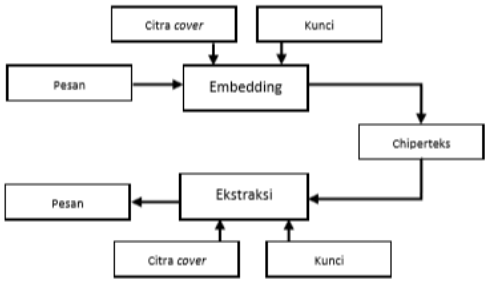
d. Variatif, memiliki banyak tingkat keamanan, Panjang kunci yang digunakan blowfish bervariasi dan bisa sangat panjang, dengan minimal 32-bit maksimal 448-bit, multiple 8 bit dengan default 128 bit. Namun, sering kali dalam menerapkan algoritma ini tidak optimal.

II. METODE PENELITIAN

A. *Kombinasi Steganografi dan Kriptografi*

1. Gambaran umum

Kombinasi dari steganografi dan kriptografi pada penelitian ini terdiri atas 2 proses, yaitu proses embedding dan ekstraksi yang dapat dilihat pada gambar 3.

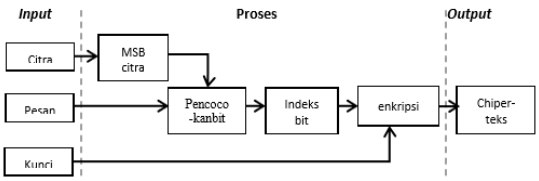


Gambar 2 Skema kombinasi steganografi dan kriptografi

Pada penelitian ini, proses embedding pada gambar diatas terdiri atas pencocokan bit dan enkripsi, hasilnya ialah cipherteks. Proses ekstraksi pada gambar 2 terdiri atas dekripsi dan rekonstruksi dan hasilnya berupa pesan.

2. Embedding

Proses embedding pada gambar 3 dapat menghasilkan indeks posisi bit, yang ada pada proses embedding adalah pesan, citra dan kunci.



Gambar 3 Proses Embedding

Langkah-langkah dalam embedding adalah sebagai berikut :

a. Memasukkan input seperti citra, pesan dan kunci ke dalam cover

b. Mengubah pesan dan citra ke bentuk biner.

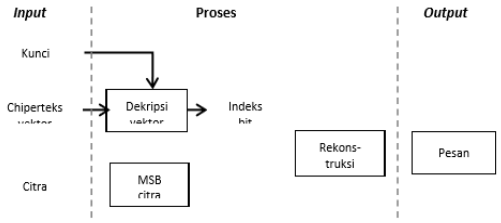
c. Mencocokkan bit pesan dan MSB citra, posisi bit yang sama lalu akan disimpan ke dalam vektor indeks bit.

d. Enkripsi vector indeks bit dengan algoritma playfair cipher, hill cipher dan blowfish.

e. Hasilnya merupakan cipherteks yang memuat vector posisi indeks bit.

3. Ekstraksi

Proses ekstraksi yang dapat dilihat pada gambar 4 memiliki tujuan untuk mengambil pesan yang ada pada cover hingga menjadi bentuk yang semula sehingga dapat diketahui isinya.



Gambar 4 Ekstraksi

Proses ekstraksi ialah sebagai berikut :

a. Memasukkan input yang merupakan cipherteks vektor, citra dan kunci.
b. Dekripsi cipherteks dengan kunci yang ada, hasilnya berupa plainteks dalam bentuk bit.
c. Melakukan rekonstruksi pesan dengan mencocokan lagi MSB citra berdasarkan vektor indeks bit.
d. Hasilnya akan berupa pesan.

III. HASIL DAN PEMBAHASAN

1.1 Pengujian Citra

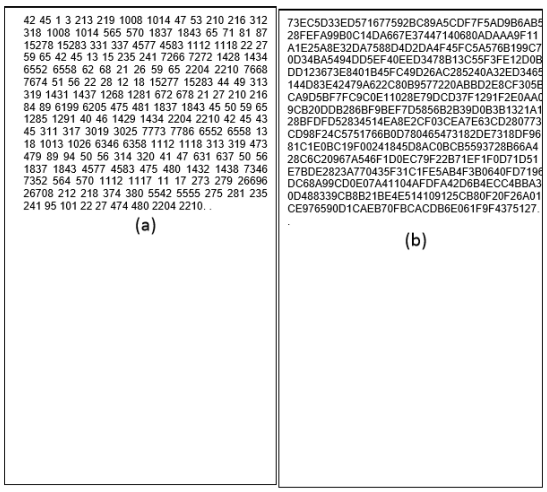
1. Embedding

Ada beberapa langkah dalam pengujian citra yaitu :

a. Pertama memilih pesan yang akan dimasukkan ke dalam gambar
b. Memilih cover citra misal gambar 6 dibawah ini

Gambar 6 Cover Citra

c. Memasukkan kunci untuk enkripsi
d. Akan muncul hasil keluaran berupa indeks bit, perbedaannya dapat dilihat pada gambar 7



Gambar 7 (a) indeks bit (b) Indek bit terenkripsi

2. Ekstraksi

Proses ini merupakan pengembalian pesan yang telah dimasukkan ke dalam citra. Proses tersebut ialah :

a. Memilih vector file yang telah dimasukkan.
b. Memilih citra yang telah dipilih sebelumnya, lihat gambar 5.
c. Menginputkan kunci
d. Ekstraksi data.

Tabel. 1 waktu proses embedding dan ekstraksi citra hitam putih

No	Citra	Embedding (detik)			Ekstraksi (detik)		
		Matching	Enkripsi	Total	Dekripsi	rekonstruksi	Total
1	lilia.bmp	1.357	24.657	26.014	24.554	0.354	24.908
2	Nas.bmp	0.326	30.21	30.536	30.341	0.437	30.778
	Rata-rata	0.8415	27.4335	28.275	27.4475	0,3955	27.843

Tabel 2. Ekstraksi dan Embedding Citra Berwarna

No	Citra	Embedding (detik)			Ekstraksi (detik)		
		Matching	Enkripsi	Total	Dekripsi	rekonstruksi	Total
1	Tas.bmp	0.876	12.546	13.422	12.984	0.249	13.233
2	Cover.bmp	0.524	11.657	12.181	11.241	0.463	11.704
3	Monyet.bmp	0.635	11.996	12.631	10.684	0.325	11.009
4	Kabel.bmp	0.663	12.067	12.73	11.540	0.825	12.365
5	Petir.bmp	1.058	13.082	14.14	14.627	1.055	15.682
	Rata-rata	0.7512	12.2696	13.0208	12.2152	0.5834	12,7986

Berdasar pengujian menunjukkan bahwa pada citra hitam putih diperoleh ratarata proses embedding 28,275 detik dengan lama waktu pencocokan bit 0,8415 detik dan enkripsi 27,4335 detik. Rata-rata proses ekstraksi yaitu 27.843 detik dengan lama dekripsi 27.4475 detik dan rekonstruksi pesan 0,3955 detik. Sedangkan pada citra warna, rata-rata proses embedding adalah 13.0208 detik dengan lama waktu untuk pencocokan bit 0.7512 detik dan enkripsi 12.2696 detik. Pada proses ekstraksi membutuhkan waktu rata-rata 12,7986 detik dengan lama waktu untuk dekripsi 12.2152 detik dan rekonstruksi pesan 0.5834 detik.

IV. KESIMPULAN

Berdasarkan penelitian, implementasi dan pengujian, maka dapat diambil kesimpulan sebagai berikut :

1. Proses steganografi seputar pencocokan bit dan rekonstruksi.
2. Proses kriptografi berupa enkripsi dan dekripsi pesan yang telah dimasukkan ke dalam citra. Kombinasi steganografi dan kriptografi pada penelitian ini dapat memperkuat dalam mengamankan data.
3. Citra berwarna maupun hitam putih dapat digunakan sebagai cover. Tetapi ada syaratnya yaitu citra tidak boleh 100% hitam atau 100% putih karena ketika citra semua hitam maka nilai bit pada citra tersebut ialah 0 dan begitu juga dengan citra semua putih nilai bitnya ialah 1.

4. Menambahkan noise pada citra dapat mengubah sebagian isi pesan dengan tingkat perubahan yang bervariatif. Pada citra hitam putih tidak terlalu berubah secara signifikan tetapi pada citra berwarna akan berubah isi pesannya.
5. Kelebihan dari metode bit matching ini ialah citra yang dimasukkan pesan tidak berubah secara kasat mata.

DAFTAR PUSTAKA

[1] Sejati, A., Studi dan Perbandingan Steganografi Metode EOF(End of File) dengan DCS(Dynamic Cell Spreading). ITB, Bandung, 2010.

[2] Aditya, Y., Pratama, A., Nurlifa, A., "Studi Pustaka untuk Steganografi dengan Beberapa Metode" SNATI 2010.

[3] Prasetyo, B., Gernomo, R., Noranita, B., "Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data " *Scientific Journal of Informatics*, vol. 1, No. 1, Mei 2014.

[4] Suhandinata, S., Rizal, R., A., Wijaya, D., O., Warren, P., Srinjiwi " ANALISIS PERFORMA KRIPTOGRAFI HYBRID ALGORITMA BLOWFISH DAN ALGORITMA RSA " *Jurteks*, Vol. VI, No. 1, hal. 1-10, 2019.

[5] Wowor, A., D., " MODIFIKASI KRIPTOGRAFI HILL CIPHER MENGGUNAKAN CONVERT BETWEEN BASE " *Seminar Nasional Sistem Informasi Indonesia*, 2013.

[6] Kurniawan, S., T., C., Dedih, Supriyadi, " Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android " *JOIN*, Vol. 2, No. 2, pp. 102-109, 2017.

[7] Munir, Rinaldi. (2018). Pengantar Kriptografi. *IF4020 Kriptografi.*

[8] Kromodimoeljo, Sentot. (2009). Teori dan Aplikasi Kriptografi, SPK IT Consulting.

[9] Ariyus, Dony. (2008). Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi. Yogyakarta: Penerbit Andi.

[10] A. Alabaichi, F. Ahmad and R. Mahmod, "Security Analysis Of Blowfish Algorithm," *International Conference on Informatics & Applications*, pp. 12-18, 2013.