

Enkripsi Citra Bitmap Menggunakan Algoritma Kompresi Lempel-Ziv-Welch (LZW)

Sudirman

Politeknik Negeri Media Kreatif PSDKU Medan
Jl. Guru Sinumba No. 6, Helvetia Timur Kec. Medan Helvetia, Kota Medan
Sumatera Utara 20124
Email : sudirman@polimedia.ac.id

Abstrak

Penggunaan data berupa file citra sudah semakin luas diberbagai bidang. Oleh karena itu pengamanan terhadap file citra dari akses orang-orang yang tidak berhak menjadi hal yang penting. Berbagai macam teknik untuk mengurangi ukuran file , termasuk juga mengamankan file telah banyak dikembangkan salah satunya adalah teknik kompresi. Teknik kompresi menjadi hal penting didalam pengolahan citra yang berukuran besar seperti citra Bitmap. Lempel Ziv Welch merupakan algoritma kompresi yang bersifat loseless yang dapat mengkompresi citra tanpa ada kehilangan unsur pixel didalamnya atau citra hasil kompresi identik dengan citra aslinya. Citra akan di enkripsi terlebih dahulu baru kemudian dilakukan teknik kompresi dengan algoritma Lempel Ziv Welch. Hasil kompresi yang dihasilkan tidak lagi dalam bentuk gambar tetapi dalam bentuk file dengan ekstensi *.mat. Perbedaan format file dari citra menjadi file yang bukan citra dapat membantu menghindari perhatian kriptanalisis.

Kata kunci: Kriptografi, Kompresi, Lempel Ziv Welch, Citra

Abstract

*The use of data in the form of image files has become more widespread in various fields. Therefore, security of image files from unauthorized persons is important. Various techniques to reduce file size, including securing files, have been developed, one of which is compression. Compression technique becomes important in processing large images such as Bitmap images. Ziv Welch seal is a loseless compression algorithm that can compress images without any loss of pixel elements in them or the resulting compression image is identical to the original image. The image will be encrypted first and then performed the compression technique using the Ziv Welch Lempel algorithm. The resulting compression is no longer in the form of images but in the form of files with the *.mat extension. The different file formats from images to non-image files can help avoid cryptanalysis*

Keywords: *Cryptography, Compression, Lempel Ziv Welch, Bitmap Image*

1. PENDAHULUAN

Citra (*image*) atau gambar merupakan salah satu bentuk multimedia yang penting. Citra menyajikan informasi secara visual dan informasi yang disajikan oleh sebuah citra lebih kaya daripada yang disajikan secara tekstual.

Citra yang disimpan atau yang akan ditransmisikan dalam bentuk *plainimage* rentan dalam bentuk penyadapan dan pencurian, seperti yang diungkapkan oleh Chin-Chen Chang [5]. Menyebutkan bahwa jumlah kejahatan dibidang teknologi informasi telah meningkat akhir-akhir ini. Tingkat keamanan menggunakan media gambar telah menjadi topik penting dalam dunia komputer. Salah satu kelemahan penggunaan media informasi media gambar adalah mudah dimanipulasi oleh pihak-pihak yang berkepentingan lain didalamnya. Terlebih jika informasi berupa *file* gambar tersebut bersifat rahasia, seperti data-data pribadi, dokumen kenegaraan atau dokumen medis rumah sakit.

Selain algoritma kriptografi yang digunakan untuk melakukan enkripsi, algoritma kompresi juga dapat berperan dalam melakukan teknik pengacakan pada citra. Proses *encoding* pada kompresi citra dapat merubah posisi *pixel-pixel* pada citra. Dimana pada proses *encoding* umumnya akan mengurangi redundansi dari data-data yang terdapat didalam citra. Sehingga posisi *pixel-pixel* pada citra akan berubah dari posisi awal sebelum dilakukan proses kompresi.

Algoritma *Lempel-Ziv-Welch* (LZW) yang merupakan algoritma kompresi *lossless* yang menghasilkan kompresi cukup baik diantara algoritma *lossless* yang ada. Algoritma ini melakukan kompresi dengan menggunakan *dictionary*, dimana fragmen-fragmen teks digantikan dengan indeks yang diperoleh dari sebuah kamus. Pendekatan algoritma ini bersifat adaptif dan efektif karena banyak karakter dapat dikodekan dengan mengacu kepada string yang telah muncul sebelumnya dalam teks [2].

Pada penelitian ini akan dilakukan penggabungan didalam melakukan pengamanan citra (*image*) yaitu teknik kriptografi dan teknik kompresi.

2. LANDASAN TEORI

Lempel Ziv Welch (LZW)

Lempel Ziv Welch (LZW) adalah algoritma kompresi *loseless* yang ditemukan oleh *Abraham Lempel, Jacob Ziv, dan Terry Welch*. Diciptakan oleh *Welch* tahun 1984 sebagai implementasi dan pengembangan algoritma LZ78 yang diciptakan oleh *Lempel dan Ziv* pada tahun 1978. Algoritma LZW dirancang untuk cepat dalam implementasi tetapi biasanya tidak optimal karena hanya melakukan analisis pada data.

Algoritma LZW melakukan kompresi dengan menggunakan *dictionary*, dimana *fragmen-fragmen* teks digantikan dengan indeks yang diperoleh dari sebuah kamus. Prinsip sejenis juga digunakan dalam kode *Braille*, dimana kode-kode khusus digunakan untuk mempresentasikan kata-kata yang ada. Pendekatan ini bersifat *adaptif* dan *efektif* karena banyak karakter bisa dikodekan dengan mengacu pada *string* yang telah muncul sebelumnya dalam teks.

Prinsip kompresi tercapai jika referensi dalam bentuk pointer dapat disimpan dalam jumlah bit yang lebih dibandingkan string aslinya. Sebagai contoh, string "ABBABABAC" akan dikompresi dengan LZW. Isi dictionary pada awal proses diset

dengan tiga karakter dasar yang ada: “A”, “B”, “C”. Tahapan proses kompresi ditunjukkan pada Tabel 2.1.

Tabel 2.1. Tahapan Proses Kompresi

Step	Posisi	Karakter	Dictionary	Output
1	1	A	[4] A B	A
2	2	B	[5] B B	B
3	3	B	[6] B A	B
4	4	A	[7] A B A	A B
5	6	C	[8] A B A C	A B A
6	9	C	---	C

Kolom posisi menyatakan posisi sekarang dari *stream* karakter dan kolom karakter menyatakan karakter yang terdapat pada posisi tersebut. Kolom *dictionary* menyatakan *string* baru yang sudah ditambahkan ke dalam *dictionary* dan nomor indeks untuk *string* tersebut ditulis dalam kurung siku. Kolom *output* menyatakan kode *output* yang dihasilkan oleh langkah kompresi.

Proses dekomposisi pada *Lempel Ziv Welch* (LZW) dilakukan dengan prinsip yang sama seperti proses kompresi. Tahapan dekomposisi ditunjukkan pada Tabel 2.2.

Tabel 2.2. Tahapan Proses Dekompresi

Step	Posisi	Output	Dictionary
1	1	A	----
2	2	B	[4] A B
3	2	B	[5] B B
4	4	A B	[6] B A
5	7	A B A	[7] A B A
6	3	C	[8] A B A C

Prinsip umum kerja algoritma Lempel Ziv Welch (LZW) adalah mengecek setiap karakter yang muncul kemudian menggabungkan dengan karakter selanjutnya menjadi sebuah string jika string baru tersebut tidak berada dalam dictionary atau belum diindekskan maka *string* baru tersebut akan diindekskan ke dalam *dictionary*. *Pseudocode* kompresi algoritma *Lempel Ziv Welch* (LZW) dapat dilihat pada Gambar 2.1.

```

1  a= NIL
2  while (ada inputan kemudian baca sebuah karakter x)
3  if (ax ada dalam kamus)
4  then a = ax
5  else
6  add ax to the dictionary
7  output indek untuk a
8  a = x
    
```

Gambar 2.1. *Pseudocode* kompresi LZW

Dalam Proses Dekompresi, algoritma LZW tidak menyimpan *string table* yang berisi indek-indek dari setiap *code word* yang dihasilkan dalam proses kompresi ke memori akan tetapi menggunakan beberapa informasi yang telah disimpan sebelumnya antara lain 256 karakter ASCII, karakter pertama dari inputan dan *code word* terakhir. Di bawah merupakan *pseudocode* dekompresi algoritma *Lempel Ziv Welch* (LZW).

```
1 read a character k
2 output k
3 w = k
4 while (read a character k )
5 dengan k dapat berupa karakter atau code
6 entry = dictionary entry for k
7 output entry
8 add w + entry[0] to dictionary
9 w = entry
```

3. METODOLOGI

3.1. Rancangan enkripsi citra digital

Rancangan proses enkripsi citra digital adalah sebagai berikut :



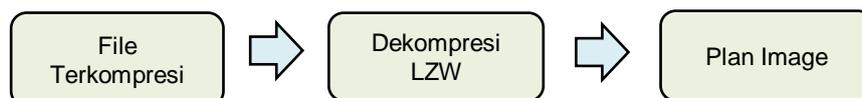
Gambar. 3.1. Skema Alur Proses Enkripsi

Berdasarkan gambar 3.1, langkah-langkah proses enkripsi yang akan dilakukan adalah sebagai berikut :

1. Penentuan *plain-image* berupa gambar atau citra yang akan dilakukan proses enkripsi.
2. Selanjutnya proses kompresi dilakukan dengan menggunakan algoritma kompresi *lampel ziv welch*.
3. Hasil dari proses diatas adalah *file* dengan ekstensi *.mat*.

3.2. Rancangan dekripsi citra digital

Rancangan proses dekripsi citra digital adalah sebagai berikut :



Gambar. 3.2. Skema Alur Proses Dekripsi

Berdasarkan gambar 3.2, langkah-langkah proses dekripsi yang akan dilakukan adalah sebagai berikut :

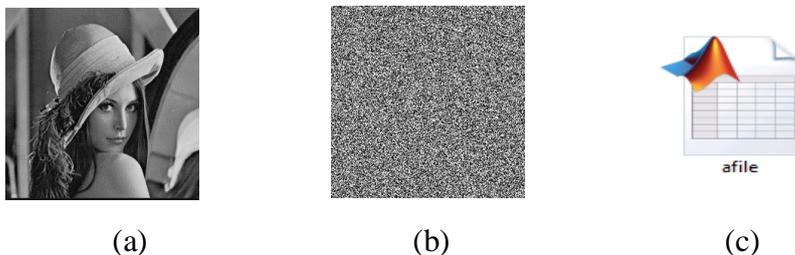
1. Pilih *file* terkompresi yang akan dilakukan proses dekompresi dan dekripsi
2. Dari *file* yang sudah dipilih akan dilakukan proses dekompresi, sehingga file akan berubah menjadi citra yang terenkripsi.
3. Selanjutnya proses dekripsi dilakukan dengan melakukan pengubahan nilai-nilai *pixel* dari *cipher-image*. *Pixel-pixel* dari *cipher-image* di XOR-kan dengan *keystream (integer)*.
4. Kemudian didapatkan citra semula (*plain-image*).

4. HASIL DAN PEMBAHASAN

Percobaan pada penelitian ini menggunakan Aplikasi Matlab R2012b dan Citra uji yang digunakan adalah citra grayscale dengan jenis citra bitmap. Citra uji yang digunakan adalah citra “lena.bmp” dengan dimensi 450 x 450 dengan ukuran 204.478 Bytes yang ditunjukkan pada gambar 4.1 (a).

4.1. Gabungan Kompresi dan Enkripsi dari Citra Digital

Pada percobaan ini akan dilakukan proses kompresi terhadap hasil enkripsi (*cipherimage*) dari algoritma *logistic map*. Proses kompresi akan dilakukan dengan menggunakan algoritma *Lempel Ziv Welch (LZW)* yang nantinya hasil dari kompresi akan disimpan dalam bentuk variabel. Variable enkripsi akan disimpan dalam direktori penyimpanan dalam bentuk *file* dengan ekstensi MAT (.mat).

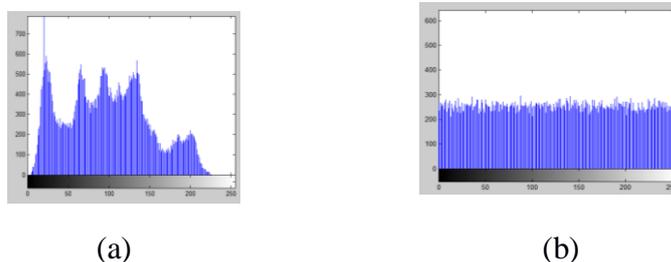


Gambar 4.1. (a) Citra Asal ; (b) *cipherimage* dengan *logistic map* ; (c) *file* hasil kompresi terhadap citra hasil enkripsi.

4.2. Analisis Histogram

Histogram merupakan salah satu fitur citra yang penting, sebab sebuah histogram memperlihatkan distribusi intensitas pixel-pixel di dalam citra tersebut. Dalam melakukan serangan dengan teknik analisis statistik, penyerang menggunakan histogram untuk menganalisis frekuensi kemunculan intensitas pixel untuk mendeduksi kunci atau pixel-pixel di dalam *plain-image*. Agar serangan dengan analisis statistik tidak dimungkinkan, maka di dalam enkripsi citra penting untuk menghasilkan histogram *cipher-image* yang tidak memiliki kemiripan secara statistik dengan histogram *plain-*

image. Oleh karena itu pixel-pixel di dalam cipher-image seharusnya memiliki distribusi yang (relatif) uniform atau ditunjukkan dengan histogram yang terlihat datar (flat).



Gambar 4.2. (a) Histogram Citra asal (lena.bmp) ; (b) Histogram Citra hasil enkripsi algoritma *Level Ziv Weld Map*.

Dari gambar 4.3. menunjukkan perubahan yang signifikan antara histogram citra asal dengan citra hasil enkripsi. Terdapat banyak perubahan intensitas pixel-pixel didalam citra yang dienkrpsi. Walaupun begitu, enkripsi hanya menggunakan algoritma logistic map saja tidak cukup aman bagi keamanan pesan citra dikarenakan kita harus menyimpan kunci yang telah dibangkitkan kedalam proses enkripsi. Hal ini membuat pesan citra mudah dipecahkan oleh pihak-pihak yang tidak berhak.

5. KESIMPULAN

Penelitian dan percobaan yang telah dilakukan menghasilkan kesimpulan sebagai berikut:

1. Hasil penelitian menunjukkan bahwa model enkripsi menggunakan
2. algoritma berbasis chaos yaitu algoritma Logistic map pada citra digital dapat menghasilkan citra acak yang sudah tidak dapat dikenali lagi.
3. Sensitivitas dari algoritma Logistic Map menunjukkan prinsip defussion, walau perbedaannya hanya 0,000000002 citra tidak kembali ke citra semula.
4. Penggunaan teknik kompresi pada citra hasil enkripsi (cipherimage) menghasilkan perubahan matrix pada citra menjadi vector, sehingga file yang dihasilkan berupa file bukan citra (.mat).

REFERENCES

- [1] Irfan,P., Prayudi, Y., & Riadi, I. 2015. Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA). *International Journal of Computer Applications* (0975 – 8887), pp. 11-16.
- [2] Neta, M.R.A. 2013. Perbandingan Algoritma Kompresi Terhadap Objek Citra Menggunakan JAVA. *Prosiding Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2013 (Semantik 2013)*, pp. 224-230.
- [3] Munir, R. 2012. Algoritma Enkripsi Citra Digital Berbasis Chaos Dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map. *Prosiding Seminar Nasional Pendidikan Teknik Infomatika (SENAPATI 2012)*, pp. 107-124.

[4] Sharma, M. 2010. Image Encryption Techniques Using Chaotic Schemes: A Review. *International Journal of Engineering Science and Technology* 2(6), pp. 2359-2363.

[5] Chang, C.-C., Hwang, M.-S & Chen, T.-S. 2001. A New Encryption Algorithm For Image Cryptosystems. *The Jurnal Of Systems And Software* 58 : 83-91.