Jurnal Mahajana Informasi, Vol.3 No. 2, 2018
e-ISSN: 2527-8290

APLIKASI PENGAMANAN FILE VIDEO MENGGUNAKAN TEKNIK KRIPTOGRAFI ALGORITMA TRANSPOSISI ZIG-ZAG

Mawati Zalukhu[1], Kharis Juliasman Hondro[2], Yuliani Susiawati Hondro[3]

[1,2,3]STMIK Budi Darma
[1]mawatizalukhu@gmail.com
[2]kharishondro@gmail.com
[3]yulianisusiawatihondro@gmail.com

ABSTRAK

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut dikirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih authenticity. Saat ini banyaknya kemudahan dalam mengunduh dan mengupload video membuat rentannya video untuk dibajak, apalagi jika video itu adalah video yang penting dan sangat rahasia maka diperlukannya suatu aplikasi yang mampu menyandikan video penting tersebut agar keamanannya dapat terjaga dari orang lain yang tidak berkepentingan, kecuali orang yang berhak. Teknik pengamanan yang digunakan penulis didalam penelitian ini, menggunakan teknink kriptografi dengan memanfaatkan algoritma zig-zag. Aplikasi dibangun menggunakan bahasa pemograman visual basic net 2008.

Kata kunci: Kriptografi, Video, Algoritma Zig-zag, Visual Basic Net 2008

I. Pendahuluan

Alat representase data salah satunya adalah video. Untuk menjaga keamanan informasi yang ada pada video. Ada beberapa teknik pengamanan yang sering di terapkan salah satu nya adalah teknik kriptografi.Dengan tujuan agar informasi tidak dapat diakses oleh orang tidak berkepetingan terhadap file video tersebut. Algoritma teknik kriptografi yang digunakan oleh penulis didalam penelitian ini adalah algoritma Zig-zag. dengan diterapkannya algoritma ini maka file video diburamkan sehingga video tidak menampilkan objek yang jelas.

Berdasarkan penelitian yang dilakukan sebelumnya oleh Susanto memaparkan bahwa untuk menjaga keamanan data yang di simpan, maka di kombinasikanlah dengan algoritma penyandian. Dengan demikian, data yang terenkripsi pada database tidak akan diketahui arti yang sebenarnya dan sulit untuk dirubah ataupun diganti (Susanto, 2017). Demikian halnya penelitian yang dilakukan oleh Hondro menyatakan pentingnya penyandian bukan hanya merubah bentuk dari data tersebut, tetapi mampu juga menghilangkan makna dari pada data itu sendiri pada saat berubah menjadi informasi bagi yang menggunakannya (Hondro, 2014). Sedangkan penelitian lain yang dilakukan oleh Zebua dalam menyandikan data mengatakan bahwa sebuah informasi penting untuk di jaga agar tidak dapat di akses dan disalahgunakan oleh orang-orang yang tidak berhak untuk mengaksesnya (T. Zebua, 2013).

II. LANDASAN TEORI

a. Kriptografi

Kata Kriptografi berasal dari Bahasa yunani: '*Cryptos'* artinya rahasia *(secret)*, sedangkan '*graphein'* artinya tulisan *(writing)*, kriptografi berarti tulisan rahasia *(secret writing)*. Ada beberapa defenisi kriptografi yang telah dikemukakan di dalam berbagai literatur (Zebua, 2018). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (R. Munir, 2006). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (J. Schneier, 1996).

Tujuan penerapan teknik kriptografi adalah untuk mengahasilkan Konfusi/pembinggungan (confusion) dari teks terang sehingga sulit untuk direkrontruksikan secara langsung tanpa menggunakan algoritma dekripsinya. Selain dari pada itu teknik kriptografi juga dapat mengahasilkan Difusi/peleburan (diffusion) dari teks terang sehingga karakteristik dari teks terang tersebut hilang sehingga dapat digunakan untuk mengamankan informasi (Zebua, 2015).

Teknik kriptografi memiliki banyak algoritma dalam mencapai tujuan di atas, di antaranya algoritma Hill Cipher, Affine Cipher, Blowfish, MUGI, CryptMT, ISAAC, DES, GOST, RC2, RC4 dan lainnya.

b. Video

Video adalah salah satu objek representasi data yang telah diolah. Bentuk data video merupakan hasil penggabungan dari pada gambar dan suara. Media video juga dapat diartikan seperangkat komponen atau media yang mampu menampilkan gambar sekaligus suara dalam waktu bersamaan.Cecep Kustandi mengungkapkan bahwa video adalah alat yang dapat menyajikan informasi, memaparkan proses, menjelaskan konsep-konsep yang rumit, mengajarkan keterampilan, menyingkat atau memperlambat waktu dan mempengaruhi sikap (P. Menezes, 1996).

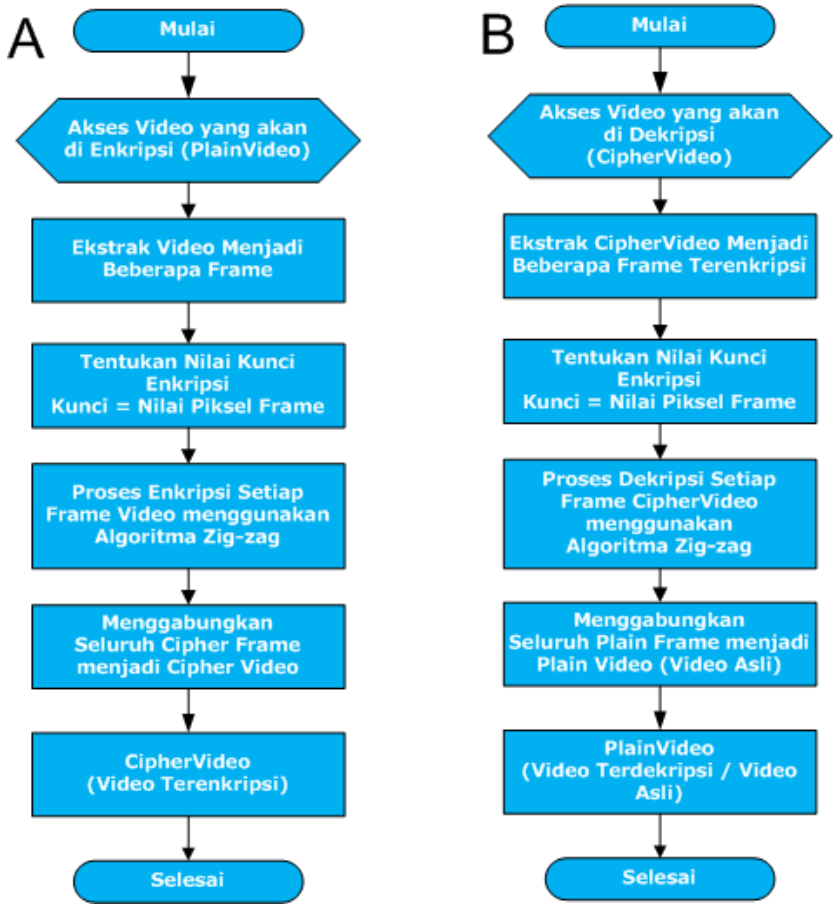
c. Algoritma Zig-zag

Algoritma Zig-Zag adalah algoritma klasik model algoritma transposisi. Pada dasarnya, teknik ini mengubah posisi dari pada nilai-nilai piksel pada data yang diamankan, dengan kata lain melakukan transpose dengan teknik permutasi atau pengacakan (scrambling) (Zebua, 2015).

III. ANALISIS SISTEM

A. Analisis Algoritma Zig-zag dalam Mengamankan File Video

Metode penyandian File Video dengan menggunakan algoritma Zig-zag yang akan dibangun menggunakan bahasa pemograman visual basic net 2008, penulis gambarkan dalam bentuk diagram flowchart, seperti pada gambar berikut ini:



Gambar 1. (A) Diagram Proses Enkripsi dan (B) Diagram Proses Dekripsi

B. Analisis Proses Enkripsi dan Dekripsi Algoritma Zig-zag Dalam Mengamankan File Video

Proses enkripsi dan dekripsi algoritma zig-zag dalam mengamankan file video. Langkah-langkah Enkripsi dan Dekripsi Zig-zag Cipher:

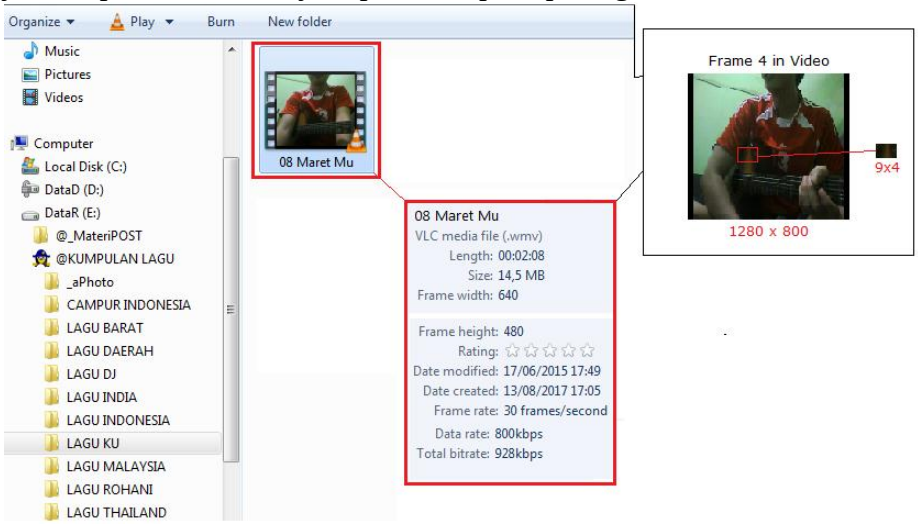
1. Bentuk Bujursangkar *(Array)* untuk menampung banyaknya karakter plaintext. Contoh: Banyak karakter plaintext = 10 , maka format array untuk menampung plaintext = 3*4 atau 4*3.
2. Tentukan Format Kunci Transposisi *(i), i = urutan baris array*
3. Proses Enkripsi dan Dekripsi Transposisi dalam Algoritma Zig-zag dapat dilakukan dengan 2 cara, boleh dilakukan secara baris (Zig-zag Baris) dan juga secara kolom (Zig-zag Kolom), pilih salah satu.
   Jika kunci di variabel dengan *"i"* maka:
   *Jika Transposisi Zig-zag Baris maka proses enkripsi : *(i , 1) (i+1, 2) (i , 3) (i+1 , 4) (i , 5)*
   *Jik Transposisi Zig-zag Kolom maka proses enkripsi : *(1, i) (2, i+1) (3 , i) (4 , i+1) (5 , i)*

IV. HASIL DAN PEMBAHASAN

A. Keluaran Enkripsi dan Dekripsi Algoritma Zig-zag

Keluaran Hasil enkrispi dengan Algoritma Zig-zag adalah Video yang buram dan tidak dapat dipahami makna gambar yang ditampilkan file video, sementara hasil dekripsi adalah kebalikan dari pada hasil enkripsi.

Pada penelitian ini penulis melakukan proses enkripsi terhadap video dengan mengambil sampel penerapan enkripsi pada frame berukuran 9 x 4 dengan jumlah piksel horizontalnya 9 piksel dan jumlah piksel vertikalnya 4 piksel, seperti pada gambar berikut ini.



Gambar 2. Format Video

Berikut ini nilai piksel dari frame 9x4 piksel:

197	178	147	197	189	147	197	178	180
167	156	168	167	156	168	167	255	168
157	167	167	177	167	255	157	167	167
167	190	183	167	190	189	167	178	185

1. Proses Enkripsi Algoritma Zig-zag

Dari nilai piksel tersebut dibentuk dalam sebuah plaintext matriks:

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	197	178	147	197	189	147	197	178	180
2	167	156	168	167	156	168	167	255	168
3	157	167	167	177	167	255	157	167	167
4	167	190	183	167	190	189	167	178	185

Kunci Format Tranposisi: 3, 1, 4, 2

Baris **pertama** transposisi nilai piksel dari nilai: (3, 1), (4, 2), (3, 3), (4, 4), (3, 5), (4, 6), (3, 7), (4, 8), (3, 9)

	1	2	3	4	5	6	7	8	9
1	197	178	147	197	189	147	197	178	180
2	167	156	168	167	156	168	167	255	168
3	157	167	167	177	167	255	157	167	167
4	167	190	183	167	190	189	167	178	185

Zig-zag Ke - 1

Offset 1	157	190	167	167	167	189	157	178	167
Offset 2									
Offset 3									
Offset 4									

Baris **kedua** transposisi nilai piksel dari nilai: (1, 1), (2, 2), (1, 3), (2, 4), (1, 5), (2, 6), (1, 7), (2, 8), (1, 9)

	1	2	3	4	5	6	7	8	9
1	197	178	147	197	189	147	197	178	180
2	167	156	168	167	156	168	167	255	168
3	157	167	167	177	167	255	157	167	167
4	167	190	183	167	190	189	167	178	185

Zig - zag Ke - 2

Offset 1	157	190	167	167	167	189	157	178	167
Offset 2	197	156	147	167	189	168	197	255	180
Offset 3									
Offset 4									

Baris **ketiga** transposisi nilai piksel dari nilai: (4, 1), (1, 2), (4, 3), (1, 4), (4, 5), (1, 6), (4, 7), (1, 8), (4, 9)

	1	2	3	4	5	6	7	8	9
1	197	178	147	197	189	147	197	178	180
2	167	156	168	167	156	168	167	255	168
3	157	167	167	177	167	255	157	167	167
4	167	190	183	167	190	189	167	178	185

Zig-zag Ke - 3

Offset 1	157	190	167	167	167	189	157	178	167
Offset 2	197	156	147	167	189	168	197	255	180
Offset 3	167	178	183	197	190	147	167	178	185
Offset 4									

Baris **keempat** transposisi nilai piksel dari nilai:

	1	2	3	4	5	6	7	8	9
1	197	178	147	197	189	147	197	178	180
2	167	156	168	167	156	168	167	255	168
3	157	167	167	177	167	255	157	167	167
4	167	190	183	167	190	189	167	178	185

Zig - zag Ke - 4

Offset 1	157	190	167	167	167	189	157	178	167
Offset 2	197	156	147	167	189	168	197	255	180
Offset 3	167	178	183	197	190	147	167	178	185
Offset 4	167	167	168	177	156	255	167	167	168

Proses enkripsi dengan algoritma Zig-zag selesai, maka hasilnya sebagai berikut:

Matriks Ciphertext

157	190	167	167	167	189	157	178	167
197	156	147	167	189	168	197	255	180
167	178	183	197	190	147	167	178	185
167	167	168	177	156	255	167	167	168

2. Proses Dekripsi Algoritma Zig-zag

Penerapan dekripsi berfungsi untuk mengembalikan tampilan video yang terenkripsi. Algoritma Zig-zag adalah algoritma kriptografi transposisi dengan kunci simetris, maka kunci transposisi untuk dekripsi sama dengan kunci transposisi pada saat enkripsi yaitu dengan format 3, 1, 4, 2.

Matriks Ciphertext

157	190	167	167	167	189	157	178	167
197	156	147	167	189	168	197	255	180
167	178	183	197	190	147	167	178	185
167	167	168	177	156	255	167	167	168

Proses Dekripsi Baris 1

Matrik Ciphertex

157	190	167	167	167	189	157	167
197	156	147	167	189	168	197	180
167	178	183	197	190	147	167	185
167	167	168	177	156	255	167	168

Matriks Plaintext

baris 1								
baris 2								
baris 3	157		167		167		157	
baris 4		190		167		189		167

Proses Dekripsi Baris 2

Matrik Ciphertex

157	190	167	167	167	189	157	167
197	156	147	167	189	168	197	180
167	178	183	197	190	147	167	185
167	167	168	177	156	255	167	168

Matriks Plaintext

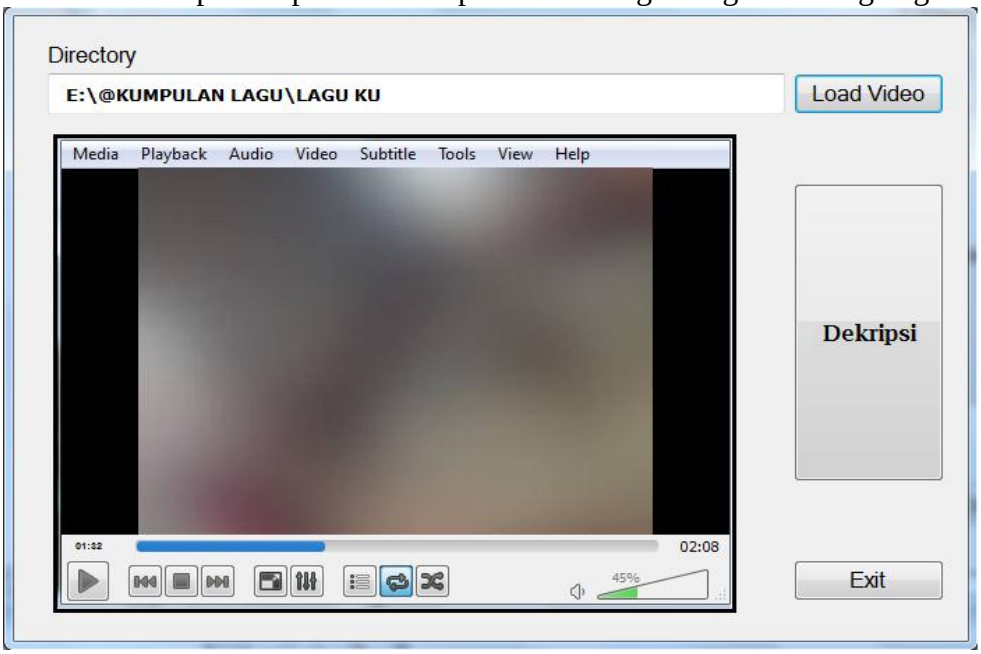
baris 1	197		147		189		197	
baris 2		156		167		168		180
baris 3	157		167		167		157	
baris 4		190		167		189		167

Lakukan hal yang sama sampai menghasil tampilan nilai piksel awal (asli) (Matriks Plaintext)

Berikut tampilan Aplikasi Enkripsi Video dengan Algoritma Zig-zag.

Gambar 3. Tampilan Form Enkripsi Video

Berikut tampilan Aplikasi Dekripsi Video dengan Algoritma Zig-zag.



Gambar 3. Tampilan Form Dekripsi Video

V. KESIMPULAN

Kesimpulan dari hasil penelitian ini, dengan dibangunnya aplikasi enkripsi ini dapat digunakan untuk mengenkripsi file video dengan tipe ekstensi *.mp4. Untuk penelitian lebih

lanjut penulis menyarankan untuk menggunakan kombinasi algoritma klasik lainnya atau menggunakan algoritma modern untuk proses enkripsi file video. Dan dapat mengaplikasikan objek video yang akan dienkripsikan dengan ekstensi yang lain seperti *.FLV, *.WMV, *.SWF, dan lain-lain

DAFTAR PUSTAKA

Susanto, "Implementasi Keamanan Data Sistem Informasi Inventory Stock Barang PT . Wings Food Menggunakan Algoritma Rivest Code 4 (RC4)," Lontar Komput., vol. 8, no. 2, pp. 77–88, 2017.

Hondro, R. K., (2014). Analisis dan Perancangan Sistem yang Menerapkan Algoritma Triangle Chain Cipher (TCC) untuk Enkripsi Record Tabel Database. Teknologi Informasi dan Komputer., vol. 3, no. 2, pp. 118-138

Hondro, R. K., (2015). Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma Zig Zag Cipher Padamobile Phone Berbasis Android. Pelita Informatika Budi Darma, vol. 10, no. 3, pp. 122-127

T. Zebua, "Diterbitkan Oleh : STMIK Budi Darma Medan ANALISA DAN IMPLEMENTASI ALGORITMA TRIANGLE CHAIN PADA PENYANDIAN RECORD DATABASE," Pelita Inform. Budi Darma, vol. III, no. 2, pp. 37–49, 2013.

Zebua, T., Hondro, R. K., & Ndruru, E. (2018). Message Security on Chat App based on Massey Omura Algorithm. IJISTECH (International Journal Of Information System & Technology), 1(2), 16.

R. Munir, Kriptografi, I. Bandung: Informatika Bandung, 2006.

J. Schneier; Bruce; Wiley, Aplied Cryptography 2nd. 1996.

P. Menezes; Alfred, J.; Orscot, Handbook of Applied Cryptography. 1996.

C. Kustandi, Media Pembelajaran Manual Dan Digital, 2nd ed. Ghalia Indonesia, 2013.

Rifki Sadiki (2012). "Kriptografi Untuk Keamanan Jaringan." Edisi.I. Yogyakarta: Andi. Hlm. 392