KRIPTOGRAFI PADA VIDEO MENGGUNAKAN METODE TRANSPOSISI

Kiki Purwanti[1)], Hamdani[2)], Anindita Septiarini[3)]

[1)]Mahasiswa Program Studi Ilmu Komputer, FMIPA, Universitas Mulawarman
[2,3)]Program Studi Ilmu Komputer, FMIPA, Universitas Mulawarman
Email : princess.qie@gmail.com

ABSTRAK

Kriptografi merupakan seni dan ilmu untuk menyandikan atau menjaga keamanan atau serta kerahasiaan pesan. Suatu pesan atau informasi yang merupakan salah satu hal penting dalam berkomunikasi yang perlu untuk dijaga kerahasiaannya. Untuk itu perlu dibuat sebuah aplikasi yang mampu mengamankan informasi baik informasi umum maupun informasi multimedia seperti video.

Metode transposisi merupakan salah satu teknik enkripsi konvensional (simetri) yang digunakan orang sejak berabad-abad lalu untuk mengamankan pesan yang dikirimkan kepada orang lain. Penerapan metode transposisi pada video dilakukan untuk melakukan pengacakan piksel yang menyusun *frame* secara horizontal dan vertikal sesuai dengan kunci simetri untuk melakukan proses enkripsi maupun dekripsi.Hal ini bertujuan untuk menyamarkan data video sehingga informasi rahasia yang terkandung di dalamnya dapat terjaga dan hanya dapat dibaca oleh pengguna yang memiliki kunci kriptografi serta aplikasi tersebut

Kata kunci : Kriptografi, Video, Enkripsi, Dekripsi, Transposisi.

PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari bagaimana supaya pesan atau dokumen itu aman, tidak bisa dibaca oleh pihak yang tidak berhak (*anauthorized persons*). Pentingnya menjaga kerahasiaan suatu informasi membuat ilmu kriptografi digunakan untuk mengamankan berbagai data, baik data informasi secara umu maupun data multimedia seperti data video pada khususnya. Perkembangan data video menimbulkan berbagai permasalahan seperti penyalahgunaan akses dan penjiplakan yang telah menimbulkan dampak serius terhadap permasalahan legal, sosial dan ekonomi.

Sehubungan dengan latar belakang maka diperlukan pengamanan *file* untuk disimpan sendiri atau untuk dikirimkan ke pihak lain yang tidak sekedar proteksi *disk* atau pengamanan secara *hardware* saja namun diperlukan salah satu teknik lain untuk pengamanan *file*. Serta hasil dari penelitian sebelumnya oleh Bangun Edmasaputra (2012) dengan judul Sistem Kriptografi pada Citra Digital Menggunakan Metode Subtitusi dan Permutasi. Serta jurnal A. Supriyanto (2011) mengenai Penyandian File Gambar dengan Metode Substitusi dan Transposisi. Dari skripsi serta jurnal tersebut penulis bermaksud untuk mengembangkan hasil penelitian sebelumnya yang hanya dapat digunakan untuk citra menjadi Kriptografi pada Video menggunakan Metode Transposisi. Dimana kriptografi yang digunakan mampu mengacak posisi piksel *frame-frame* yang menyusun video.

Metode Penyandian Transposisi

Teknik transposisi pada dasarnya adalah membuat *ciphertext* dengan menggantikan posisi objek-objek *plaintext* tanpa menggantikan objek *plaintext* tersebut, jadi pada teknik transposisi ini tidak diperlukan karakter lain. Pada teknik transposisi ini pembuatan *ciphertext* dilakukan dengan pembacaan nilai matrix pada kolom per kolom sesuai dengan kunci yang digunakan (Kurniawan, 2004.).

Teknik transposisi karakter sebagai contoh *cipher* dari *plaintext* "saya sedang belajar kriptografi" pada tabel 1.

Tabel 1. Contoh Metode Transposisi

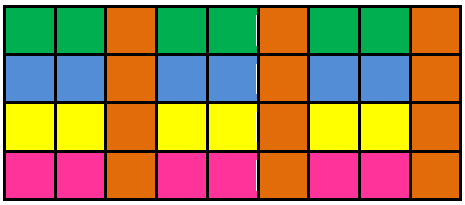
Kunci	4	3	1	5	2	6
Plain text	S	A	Y	A	S	E
	D	A	N	G	B	E
	L	A	J	A	R	K
	R	I	P	T	O	G
	R	A	F	I	Y	Z

Plaintext disusun ke kanan kemudian ke bawah. kuncinya adalah 4 3 1 5 2 6, sehingga keluaran *cipher* mengikuti kunci menurun ke bawah : ynjpf sbroy aaaia sdirr agati eekgz. Karakter y dan z ditambahkan untuk menutupi jejak

bahwa jumlah karakter yang sebenarnya hanya sebanyak 4 kolom sehingga lebih mempersulit analisis *cipher*.

Analisis Proses Enkripsi

Enkripsi ialah melakukan penyamaran data dengan menggunakan kunci yang disebut proses enkripsi. Kunci yang digunakan berupa alfanumerik (a-z, A-Z, 0-9). Contoh proses enkripsi pada *frame* berukuran 9x4 piksel pada Gambar 1.



Gambar 1. *Frame* 9x4

Proses pengulangan kunci sesuai dengan jumlah kolom *frame* video untuk transposisi horizontal ditampilkan pada Tabel 2.

Tabel 2. Kunci dan hasil pengulangan kunci sesuai kolom

Kunci Awal	K	R	I	P	-	-	-	-	-
Pengulangan kunci sesuai jumlah Kolom *Frame*	K	K	R	R	I	I	P	P	P

Pengulangan dilakukan perhuruf hingga didapat panjang sesuai. Jika pengulangan pada tiap huruf sudah dilakukan dan jumlah kunci belum sesuai dengan panjang kolom maka sisa pengulangan akan dilakukan dari huruf yang terakhir seperti ada tabel 3. Setelah itu kunci akan dikelompokkan berdasarkan jenis huruf atau angka yang menyusun kunci. Proses selanjutkan yaitu mengindekskan posisi awal kunci dan posisi *frame*, terdapat pada Tabel 3.

Tabel 3. Posisi awal kunci dan *frame*

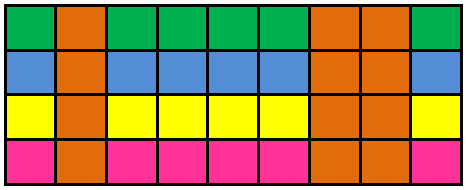
Pengulangan Kunci	K	K	R	R	I	I	P	P	P
Posisi awal *frame*	1	2	3	4	5	6	7	8	9
Frame Awal / *Plain frame*									

Selanjutnya akan diperlihatkan proses enkripsi dengan transposisi secara horizontal yang akan dijabarkan pada Tabel 4.

Tabel 4. Proses Enkripsi dengan transposisi horizontal

Pengulangan Kunci	K	K	R	R	I	I	P	P	P
Kunci Terurut	I	I	K	K	P	P	P	R	R
Posisi awal *frame*	1	2	3	4	5	6	7	8	9
Frame Awal / *Plain frame*									

Pada tabel 4 kunci yang terulangan diurutkan berdasarkan alfanumerik diikuti dengan posisi *frame* per kolom sehingga terbentuk *frame* baru yang telah terenkripsi seperti pada Gambar 2.



Gambar 2. *Frame* transposisi horizontal

Proses selanjutnya enkripsi transposisi vertikal. *Frame* yang digunakan ialah *frame* yang telah dilakukan proses transposisi horizontal. Proses pertama ialah menyamakan jumlah kunci dengan jumlah baris pada *frame* piksel. Dilanjutkan dengan mengindekskan posisi *frame* secara vertikal sesuai dengan kunci yang dipakai sesuai pada Tabel 5.

Tabel 5. Posisi Kunci Terhadap Posisi *Frame* secara Vertikal

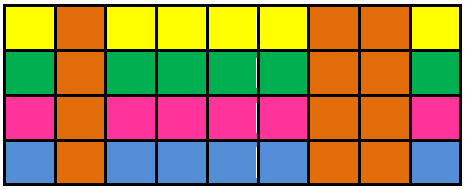
Kunci	Posisi Awal *Frame*	Posisi *frame*
K	1	
R	2	
I	3	
P	4	

Selanjutnya dilakukan transposisi vertikal dengan perpindahan kunci yang diikuti *frame* secara vertikal sesuai urutan alfanumerik ditabel 6.

Tabel 6. Enkripsi Transposisi Vertikal

Kunci		Kunci Terurut	Posisi *Frame*	Posisi *frame*
K		I	1	
R		K	2	
		P	3	
P		R	4	

Pada Gambar 3 dapat dilihat bahwa terjadi perubahan posisi warna piksel yang menyusun *frame* baik secara horizontal maupun vertikal sesuai dengan kunci yang digunakan.



Gambar 3. *Frame* Hasil Enkripsi Horizontal dan Vertikal

Analisis Proses Dekripsi

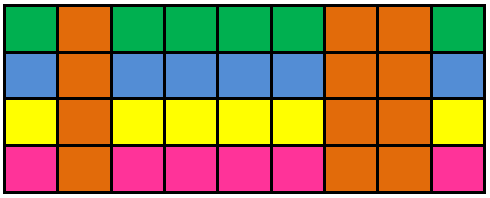
Dekripsi merupakan proses kebalikan dari proses enkripsi. Dari proses enkripsi akan dihasilkan *cipher frame* dan untuk mengembalikan *frame* tersebut kembali ke *plain frame* awal maka harus dilakukan proses dekripsi dengan memasukkan kunci yang sesuai dengan kunci awal saat melakukan enkripsi. Proses pertama dekripsi yaitu proses pembacaan kunci yaitu dengan mengembalikan huruf yang sesuai urutan abjad menjadi kunci awal enkripsi.

Dekripsi pertama yang dilakukan adalah proses transposisi secara vertikal. Proses dimulai dengan menyamakan jumlah kunci dengan jumlah baris pada *cipher frame* pada Tabel 7.

Tabel 7. Dekripsi Transposisi Vertikal

Kunci Terurut		Kunci awal	Posisi Frame	Posisi *frame*
I		K	1	
K		R	2	
P		I	3	
R		P	4	

Proses pengembalian kunci menjadi kunci awal diikuti oleh perpindahan piksel per baris seperti Gambar 4.



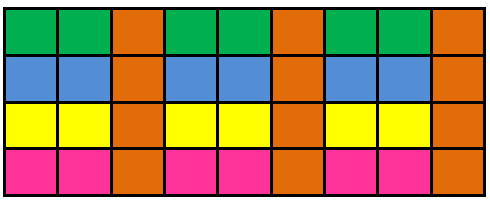
Gambar 4. *Frame* Dekripsi Vertikal

Selanjutnya proses dekripsi kedua yaitu dekripsi berdasarkan transposisi secara horizontal. Proses yang dilakukan yaitu menyamakan jumlah kunci dengan jumlah kolom pada *frame* dengan melakukan perulangan pada masing-masing huruf pada kunci. Setelah panjang kunci sesuai maka *frame* dengan kunci terurut ditransposisi kembali menjadi *frame* dengan kunci awal diikuti oleh piksel *frame* per kolom. Proses dekripsi secara horizontal dapat dilihat pada Tabel 8.

Tabel 8. Dekripsi Transposisi Horizontal

Kunci Terurut	I	I	K	K	P	P	P	R	R
Kunci Awal	K	K	I	I	R	R	P	P	P
Posisi *Frame*	1	2	3	4	5	6	7	8	9
Frame									

Dari hasil transposisi horizontal maka akan dihasilkan *frame* dekripsi secara horizontal dan vertikal seperti Gambar 5. *Frame* yang dihasilkan dari proses dekripsi kembali seperti *frame* asli sebelum dilakukan proses dekripsi. Oleh karena itu *frame* hasil dekripsi disebut *plain cipher* atau *frame* terdekripsi.

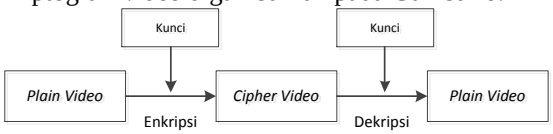


Gambar 5. *Plain frame* atau *Frame* terdekripsi

Deskripsi Sistem

Sistem kriptografi video menggunakan metode transposisi merupakan salah satu teknik mengamankan data dari pihak yang tidak berwenang, data multimedia khususnya berupa data video. Proses enkripsi dan dekripsi yang dilakukan

yaitu dengan metode transposisi sesuai dengan kunci yang dimasukkan pengguna. Sistem kriptografi video digambarkan pada Gambar 6.



Gambar 6. Sistem Kriptografi Video

Proses transposisi dilakukan dengan mengacak posisi pada piksel-piksel yang menyusun *frame* sesuai dengan kunci yang dimasukkan pengguna. Proses transposisi dilakukan secara 2 tahap yaitu dimulai dengan transposisi horizontal dan transposisi vertikal untuk enkripsi maupun dekripsi. Tahap berlapis dilakukan agar piksel pada potongan *frame* semakin teracak sehingga data semakin tersamarkan.

Perancangan Program

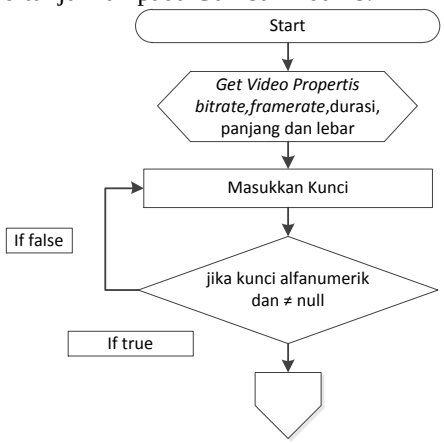
Perancangan program pada sistem kriptografi pada video dengan metode transposisi menggunakan *flowchart* untuk rincian proses pada aplikasi.

Proses Utama

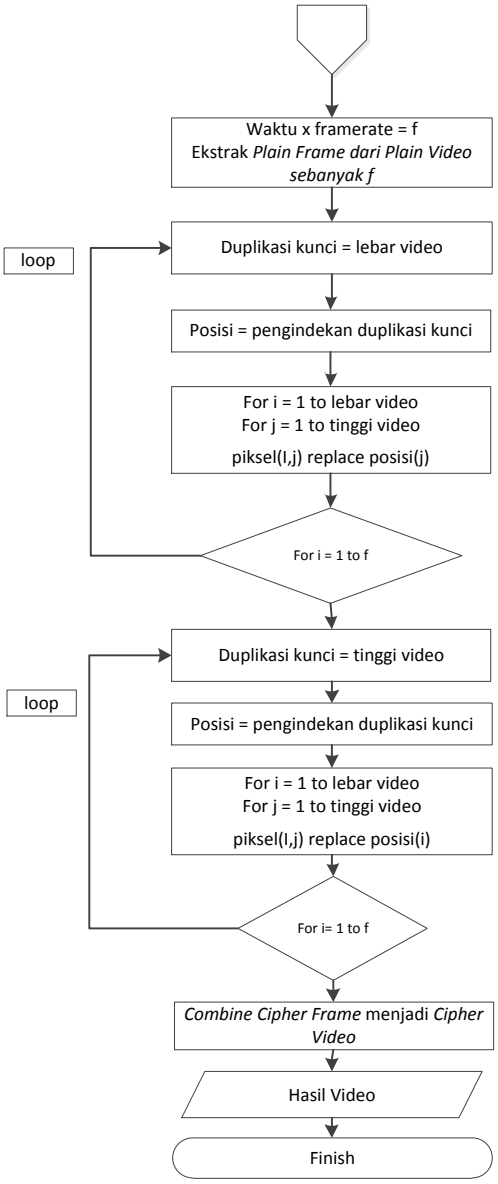
Proses utama pada aplikasi kriptografi video menggunakan metode transposisi yaitu proses untuk melakukan proses utama yaitu proses enkripsi dan proses dekripsi. Dimana pengguna dapat memasukkan data berupa *plain video*, *cipher video* disertai dengan kunci rahasia. Selanjutnya data yang masuk pada sistem akan dilakukan proses kriptografi video yaitu enkripsi dan dekripsi menggunakan metode Transposisi yang hasil keluarannya berupa *cipher video* dan *plain video*.

Proses Enkripsi

Proses enkripsi dapat dilihat aliran data pada sistem aplikasi kriptografi video menggunakan metode transposisi pada *flowchart* proses enkripsi yang ditunjukkan pada Gambar 7 dan 8.



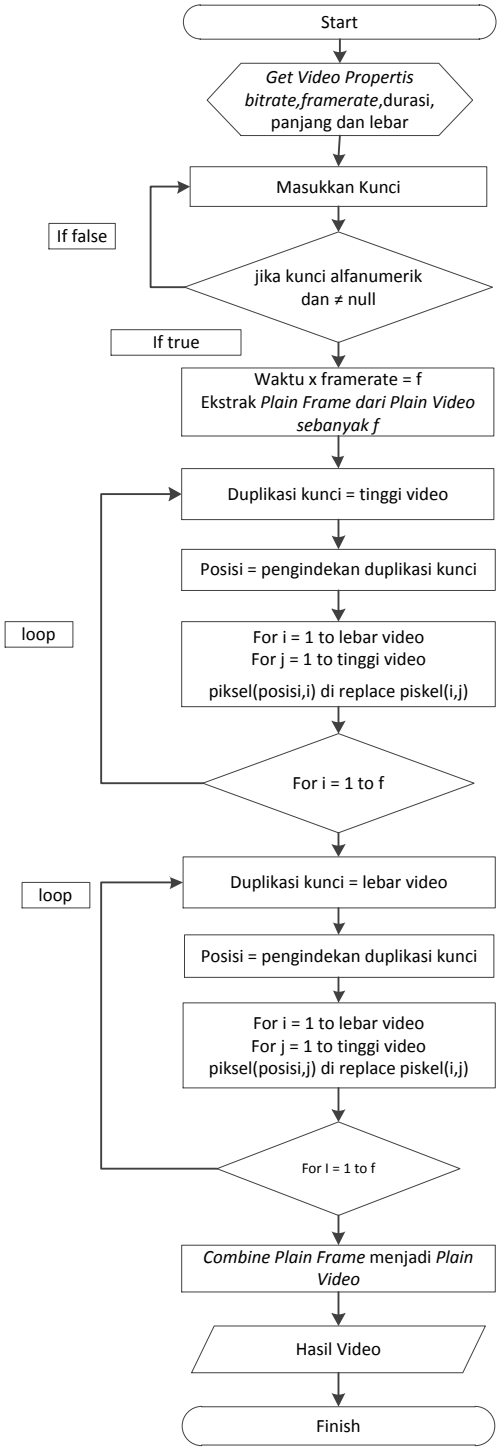
Gambar 7. Flowchart Enkripsi Bagian 1



Gambar 8. *Flowchart* Enkripsi Bagian 2

Proses Dekripsi

Proses dekripsi dapat dilihat aliran data pada sistem aplikasi kriptografi video menggunakan metode transposisi. Dan untuk proses lebih rinci dari sistem tersebut dapat dilihat pada *flowchart* proses dekripsi pada Gambar 9.



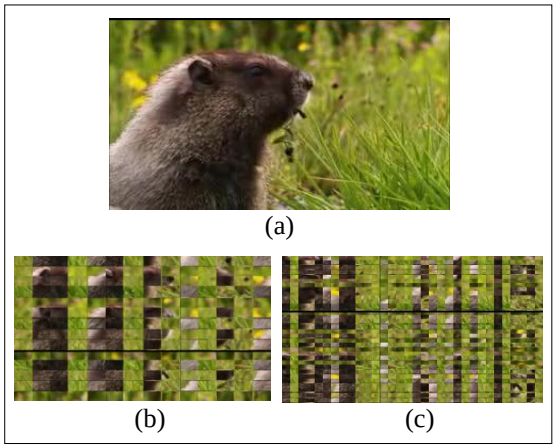
Gambar 9. *Flowchart* Dekripsi

Pengujian Sistem

Pengujian sistem pada kriptografi video memfokuskan pengujian pada tingkat keberhasilan melakukan proses enkripsi dan dekripsi, apakah video awal dapat dikenali saat sudah dilakukan proses enkripsi dengan pengacakan piksel pada *frame* dan video dapat kembali seperti video awal sehingga informasi di dalamnya dapat dipergunakan kembali. Pengujian sistem yang dilakukan berdasarkan beberapa perbandingan parameter yang menyusun video.

Pengujian Berdasarkan Kunci

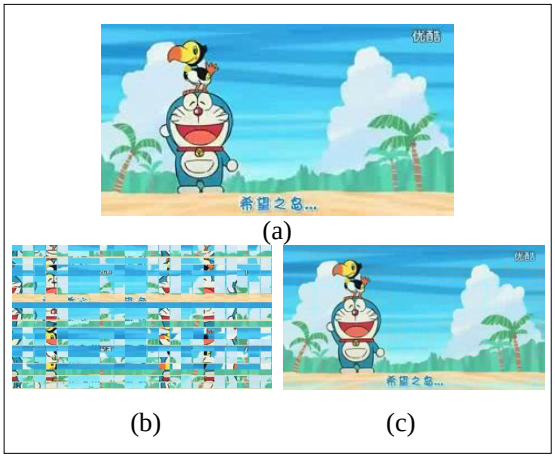
Pengujian pertama dilakukan dengan melihat hasil pengacakan pada *frame* dengan membandingkan jumlah kunci yang digunakan untuk melakukan proses enkripsi maupun dekripsi. Pada Gambar 10 diperlihatkan hasil enkripsi berdasarkan jumlah kunci yang digunakan untuk melakukan proses enkripsi. Dari ke dua hasil enkripsi dapat dilihat bahwa hasil enkripsi dengan kunci yang lebih panjang menghasilkan *cipher frame* yang lebih teracak sehingga semakin sulit dikenali dari *frame* awal dibandingkan dengan *cipher frame* dengan kunci yang lebih sedikit.

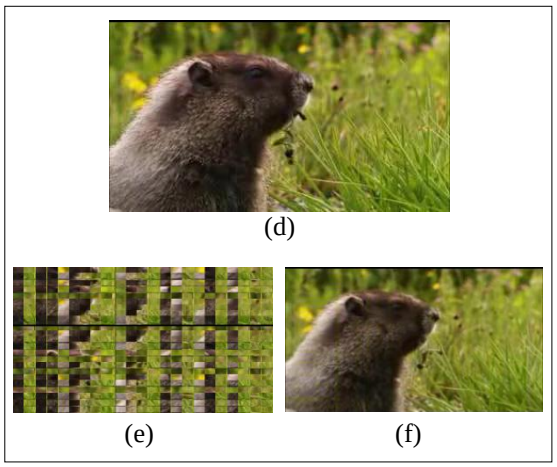


Gambar 10. (a) *plain frame*, (b)*cipher frame* kunci ‘s7’, (c) *cipher frame* kunci ‘kriptografivideo2007’

Pengujian Berdasarkan Format *Real Video* dan Animasi

Pengujian selanjutnya dilakukan berdasarkan format video yang akan dilakukan proses kriptografi. Pengujian dilakukan pada *real video* dan animasi yang memiliki ukuran *frame* video serta panjang kunci yang sama.





(d)

(e) (f)

Gambar 11. (a)*plain frame* animasi (b)*cipher frame* animasi (c)hasil *plain frame* animasi, (d)*plain frame* real video, (e)*cipher frame* real video, (f) hasil *plain frame* real video

Dari Gambar 11 mengenai perbandingan hasil *frame* proses kriptografi dengan metode transposisi pada video animasi dan *real video* dapat diketahui bahwa hasil enkripsi dan dekripsi berupa *plain frame* yang dihasilkan terlihat bahwa video dengan format *real video* memiliki *plain frame* yang lebih baik dibandingkan dengan *plain frame* dengan video animasi. Pada *plain frame* animasi terlihat jelas garis-garis yang membentuk potongan hasil proses enkripsi sebelumnya. Sedangkan pada *plain frame real video* hasil garis-garis potongan terlihat samar.

Pengujian Waktu Proses Enkripsi dan Dekripsi

Pengujian dilakukan untuk melihat waktu yang dibutuhkan untuk melakukan proses enkripsi maupun proses dekripsi berdasarkan ukuran *frame* video (dalam piksel). Hasil pengujian terdapat pada Tabel 9.

Tabel 9. Pengujian Waktu Proses Enkripsi dan Dekripsi

Ukuran Video	Durasi (detik)	FPS (fps)	Waktu Proses (menit)	
			Enkripsi	Dekripsi
320 x 240	05:00	15	01:27.57	01:23.50
		30	02:49.79	02:47.37
400 x 240	05:00	15	01:48.87	01:47.62
		30	03:39.12	03:34.07
480 x 320	05:00	15	02:51.24	02:55.49
		30	05:38.49	05:50.37
480 x 360	05:00	15	03:02.46	03:07.03
		30	06:04.85	06:13.05
720 x 480	05:00	15	06:08.63	06:04.74
		30	12:17.83	12:08.06

Berdasarkan pengujian waktu proses melakukan proses enkripsi dan dekripsi menggunakan metode transposisi, maka dapat dilihat hasil pada tabel bahwa lama waktu yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi berbanding lurus dengan banyaknya fps yang menyusun video, besarnya ukuran *frame* video serta durasi dari video.

KESIMPULAN

Kesimpulan penelitian mengenai kriptografi video menggunakan metode transposisi antara lain :

1. Kriptografi pada video menggunakan metode transposisi dilakukan dengan melakukan pengacakan piksel pada tiap *frame* yang menyusun video.
2. Teknik pengenkripsian dengan metode transposisi yang digunakan meliputi dua langkah yaitu transposisi secara horizontal dan transposisi secara vertikal.
3. Parameter yang menunjang keberhasilan dalam melakukan proses kriptografi video dengan metode transposisi antara lain jenis video yang digunakan serta besarnya *bitrate* suatu video.
4. Kriptografi transposisi kurang cocok digunakan untuk *file* yang memiliki kualitas warna rendah seperti film animasi.
5. Berdasarkan penelitian diketahui bahwa lama proses untuk melakukan proses kriptografi video menggunakan metode transposisi ditentukan oleh besar *frame* video, fps video dan durasi video.

DAFTAR PUSTAKA

[1]. Ahman, U. 2005. *Pengolahan Citra Digital dan Teknik Pemrogramannya.* Yogyakarta : Graha Ilmu.

[2]. Ariyus, D. 2006. *Computer Security*. Yogyakarta : Penerbit Andi.

[3]. Edmasaputra, B. 2012. *Sistem Kriptografi pada Citra Digital Menggunakan Metode Subtitusi dan Permutasi.* Skripsi Ilmu Komputer Universitas Mulawarman. Samarinda

[4]. Kurniawan, Y. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung : Penerbit Informatika

[5]. Munir, R. 2006. *Kriptografi*. Bandung : Penerbit Informatika.

[6]. Munir, R. 2004. *Pengolahan Citra Dengan Pendekatan Algoritmik*. Bandung : Informatika,

[7]. Rosa, A. 2011. *Rekayasa Perangkat Lunak*. Bandung :Modula.

[8]. Supriyanto, A. 2008. *Penyandian File Gambar dengan Metode Substitusi dan Transposisi.* Jurnal Teknologi Informasi Dinamik. Volume XIII, No.2, P : 88-97