MODIFIKASI VIDEO *ENCRYPTON ALGORITHM* UNTUK MENINGKATKAN TINGKAT KEAMANANNYA

Ari Moesriami Barmawi[1], Nurjanah Syakrani[2], Faren[3], Heri Budianto[4]
[1], [2], [3], [4] Jurusan Teknik Komputer Politeknik Negeri Bandung

VIDEO ENCRYPTION ALGORITHM MODIFICATION TO IMPROVE SECURE LEVEL

Abstract: Nowadays, information exchange through electronic media becomes one of communication ways which is frequently used for communicating with each other. Since there are information which have to be kept secret during the transmission while the communication line can not prevent the information against the eavesdropper, impersonating, man in the middle attack, etc, then the way to keep the information secret should be considered. One of methods for keeping the information secret is cryptography. There are many cryptosystems which have been proposed for preventing information against attacker. Two of them are Video Encryption Algorithm (VEA) and Data Encryption Standards (DES) which can be used for encrypting information in either visual or text. However, both cryptosystems still have weaknesses. VEA is less secure than DES, while DES needs more time for processing the video/picture encryption compared with VEA. This paper introduce a cryptosystem for encrypting video/picture which needs less time for encrypting video/picture but has equal security as DES. In other words, the proposed cryptosystem is more secure than VEA. This cryptosystem is a development of both DES and VEA. Based on analysis we demonstrated that our approach confirmed those above advantages.

Keywords: Kriptografi, Video Encryption Algorithm (VEA), Data Encryption Standards (DES), Random Number, Permutasi

Dewasa ini pertukaran informasi melalui media elektronik menjadi salah satu hal yang sangat sering dilakukan saat beberapa individu berkomunikasi antara satu sama lain. Mengingat sebagian informasi harus dijaga kerahasiaannya selama proses pengiriman, sementara media komunikasi yang digunakan adalah media umum yang rentan terhadap penyadapan, pemalsuan, dan lain-lain, maka keamanan informasi saat pertukaran informasi tersebut berlangsung perlu diperhatikan dengan seksama. Salah satu metode pengamanan yang sering digunakan adalah kriptografi. Informasi yang dipertukarkan dapat berupa informasi teks atau gambar, bahkan suara. Berbagai sistem kriptografi sudah pernah diajukan baik untuk

Alamat Korespondensi:
Ari Moesriami Barmawi, Jurusan Teknik Komputer Politeknik Negeri Bandung
Telepon : (022) 2013789; Fax. (022) 2013889

teks atau gambar, tetapi khusus untuk gambar diperlukan sistem kriptografi yang membutuhkan waktu eksekusi cepat mengingat ukuran gambar jauh lebih besar daripada teks. Dalam rangka mengamankan gambar, Shi dan Bhargava mengajukan sebuah sistem kriptografi khusus untuk gambar yang diberi nama *VEA* (Shi and Bhargava, 1998a; 1998b). Walaupun demikian, kekuatannya tidak sebaik sistem kriptografi lainnya, seperti *DES* (Stinson, 1995). Bila *DES* digunakan untuk mengamankan gambar, diperlukan waktu eksekusi yang cukup panjang. Dengan demikian, diperlukan suatu sistem kriptografi yang memiliki kekuatan pengamanan yang baik, tetapi tidak membutuhkan waktu eksekusi yang tinggi. Untuk itu, pada makalah ini diajukan sistem kriptografi yang merupakan pengembangan dari *VEA* dan *DES*. Pembahasan tentang sistem ini juga akan dilengkapi dengan penerapannya pada protokol kriptografi yang digunakan.

DES* dan *VEA

DES adalah sistem kriptografi simetrik (proses enkripsi dan dekripsi sama) yang dikategorikan dalam *"block cipher"*. Pada sistem ini digunakan kunci yang memiliki panjang 64 bit, tetapi panjang kunci sesungguhnya adalah 56 bit sementara 8 bit sisanya digunakan untuk pemeriksaan bit paritas. Kunci dengan panjang 56 bit ini digunakan untuk membuat 16 buah kunci turunannya dengan ukuran 48 bit melalui 16 putaran proses. Adapun caranya adalah dengan mengambil 48 bit dari kunci tersebut pada posisi tertentu, kemudian dijadikan masukan bagi proses putaran pertama, sehingga dihasilkan kunci turunan pertama sepanjang 64 bit. Kunci turunan pertama ini, kemudian akan menjadi masukan bagi proses putaran kedua untuk menghasilkan kunci turunan ke dua sepanjang 64 bit. Hal ini berlaku berulang hingga putaran ke enam belas. Proses enkripsi data sepanjang 64 bit dilakukan dengan 16 putaran pula dengan memanfaatkan 16 kunci yang telah dibuat. Berdasarkan proses yang dilakukan tampak bahwa tingkat keamanan sistem kriptografi *DES* (Stinson, 1995) cukup tinggi walaupun perlu disertai penam-bahan panjang kunci sejalan dengan peningkatan kinerja perangkat keras komputer. Sebagai contoh, dengan kunci sepanjang 128 bit akan diperoleh tingkat keamanan yang tinggi sampai tahun 2121. Walaupun demikian, bila hal ini diterapkan pada gambar akan membutuhkan waktu eksekusi yang cukup tinggi.

Sistem kriptografi lain yang pernah diusulkan untuk mengamankan gambar yang berupa video adalah sistem yang diajukan oleh Shi dan Bhargava yaitu *VEA*, sebenarnya diciptakan untuk melakukan pengamanan informasi yang berupa gambar video berformat *Moving Picture Experts Group* (*MPEG*) tetapi sebenarnya algoritma sistem kriptografi ini juga dapat diterapkan pada gambar berformat lainnya. Sistem kriptografi ini ditujukan untuk menjamin agar informasi yang dikirimkan tidak dapat dibuka oleh pihak yang tidak berhak membaca. Gagasan dasar algoritma ini adalah melakukan proses pengamanan informasi dengan memanfaatkan kunci rahasia. Secara umum, algoritma sistem kriptografi *VEA* sangat sederhana yaitu meng-*XOR*-kan kunci rahasia dengan setiap koefisien *Discrete Cosine Transform* (*DCT*) yang terdapat pada *MPEG*.

Adapun secara lebih rinci dapat dijelaskan sebagai berikut. Misalnya sebuah informasi (*plain-text*) berupa video *S* yang dapat direpresentasikan dalam Persamaan 1.

$$S=s_1 s_2 s_3 \ldots s_m \ldots \quad (1)$$

dengan s_i adalah seluruh koefisien *Alternating Current* (*AC*) (informasi) dan *Direct Current* (*DC*) (nilai rata-rata *brightness*) yang akan diamankan (dienkripsi) menggunakan kunci *K* yang dapat direpresentasikan pada Persamaan 2.

$$K=k_1k_2k_3...k_m \quad (2)$$

dengan k_i adalah bit ke-*i* dari kunci rahasia yang akan digunakan. Hasil enkripsinya $E_k(S)$ dapat dilihat pada Persamaan 3.

$$E_k(S)=(k_1 \oplus s_1)(k_2 \oplus s_2)(k_3 \oplus s_3)...(k_m \oplus s_m) \quad (3)$$

Dengan demikian, sistem kriptografi ini rentan terhadap penyerangan *plaintext*, yaitu bila seseorang mengetahui *plaintext* dan mengetahui hasil enkripsi *plaintext* tersebut, maka kunci yang digunakan dapat dengan mudah diperoleh.

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa permasalahan pokok dalam mengamankan informasi berupa gambar adalah bahwa bila dibutuhkan tingkat keamanan yang tinggi, maka sebagai konsekuensinya diperlukan pula waktu eksekusi yang tinggi.

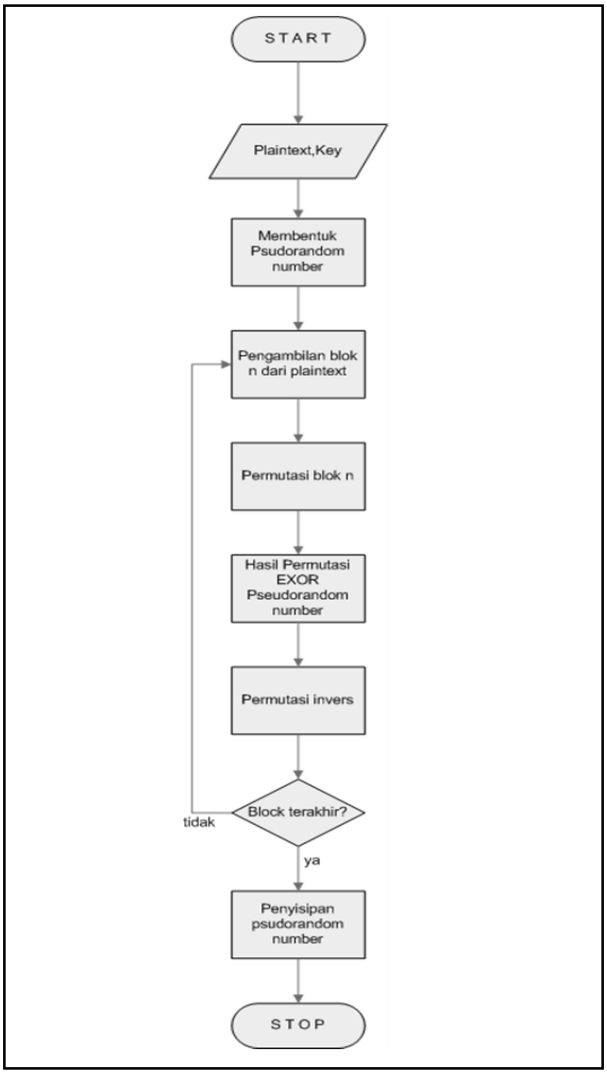
METODE

Sistem Kriptografi yang Diusulkan (Modifikasi *VEA*)

VEA sebenarnya merupakan sistem kriptografi dengan waktu eksekusi pendek, tetapi tingkat keamanannya relatif rendah. Untuk itu diusulkan sistem kriptografi yang mempunyai kekuatan lebih tinggi dari *VEA* tetapi membutuhkan waktu eksekusi lebih kecil dari *DES*.

Pada sistem kriptogafi yang dikembangkan ini diusulkan adanya beberapa pengembangan diantaranya kunci yang disembunyikan dalam informasi yang sudah diamankan (*"encrypted text"*), pemanfaatan permutasi, serta proses *XOR*. Perbedaan utama antara sistem kriptografi yang diusulkan pada makalah ini dengan *VEA* terletak pada penggunaan kunci dalam proses enkripsi serta proses pembuatan kunci. Bila pada *VEA*, kunci langsung di-*XOR*-kan dengan komponen *DCT* (*plaintext*), maka pada sistem kriptografi yang diusulkan kunci tidak langsung di-*XOR*-kan dengan *plaintext*. Di samping itu, perbedaan lainnya adalah penyelipan kunci pada pesan yang telah dienkripsi (*cyphertext*).

Prosedur pengamanan informasi (enkripsi) dari sistem ini secara lengkap dapat dilihat pada Gambar 1.



Gambar 1 Diagram Alir Proses Enkripsi

Tabel 1 Permutasi dan Permutasi Invers
(a) Permutasi
(b) Permutasi Invers

116	100	84	68	52	36	20	4
120	104	88	72	56	40	24	8
124	108	92	76	60	44	28	12
128	112	96	80	64	48	32	16
115	99	83	67	51	35	19	3
119	103	87	71	55	39	23	7
123	107	91	75	59	43	27	11
127	111	95	79	63	47	31	15
114	98	82	66	50	34	18	2
118	102	86	70	54	38	22	6
122	106	90	74	58	42	26	10
126	110	94	78	62	46	30	14
113	97	81	65	49	33	17	1
117	101	85	69	53	37	21	5
121	105	89	73	57	41	25	9
125	109	93	77	61	45	29	13

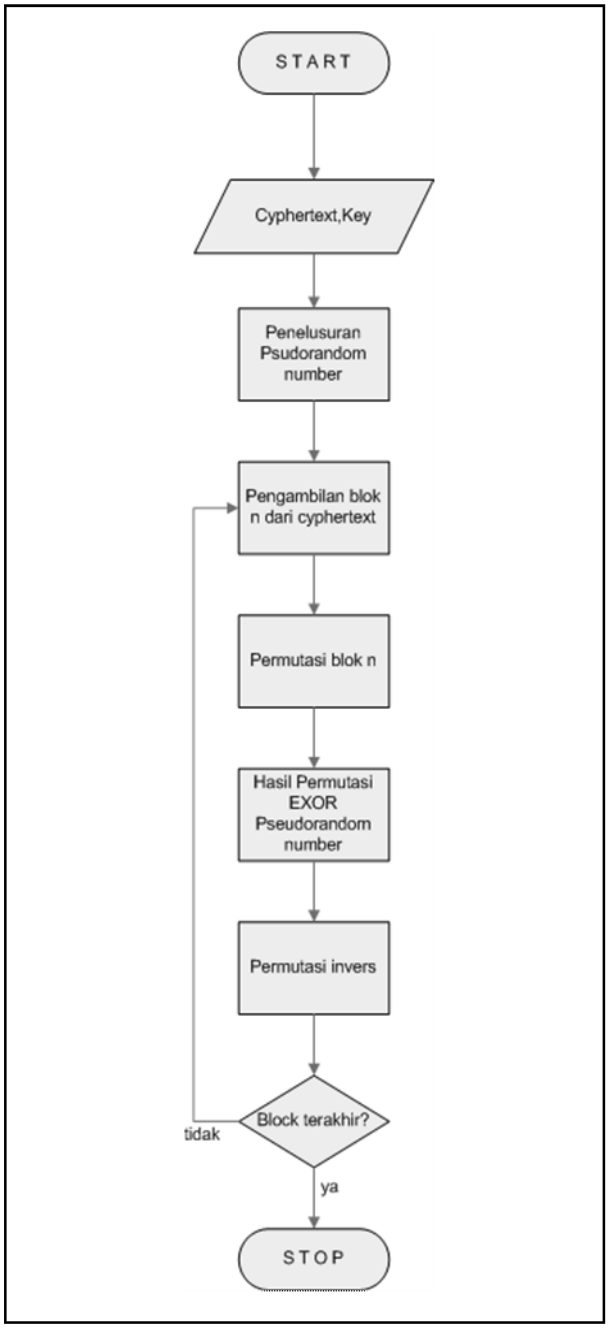
(a)

104	72	40	8	112	80	48	16
120	88	56	24	128	96	64	32
103	71	39	7	111	79	47	15
119	87	55	23	127	95	63	31
102	70	38	6	110	78	46	14
118	86	54	22	126	94	62	30
101	69	37	5	109	77	45	13
117	85	53	21	125	93	61	29
100	68	36	4	108	76	44	12
116	84	52	20	124	92	60	28
99	67	35	3	107	75	43	11
115	83	51	19	123	91	59	27
98	66	34	2	106	74	42	10
114	82	50	18	122	90	58	26
97	65	33	1	105	73	41	9
113	81	49	17	121	89	57	25

(b)

Pada Gambar 1 terlihat bahwa prosedur enkripsi diawali dengan pembuatan bilangan acak *(Pseudo-random Number)* (Knuth, 1998) menggunakan kunci sebagai *seed*. Setelah itu *plaintext* dibagi dalam beberapa *block* yang panjangnya 128 bit, dan kemudian dipermutasikan sesuai tabel permutasi seperti yang tampak pada Tabel 1(a). Bilangan acak yang telah dibuat di-*XOR*-kan dengan hasil *block* yang telah dipermutasikan untuk kemudian dilakukan permutasi invers seperti yangditunjukkan pada Tabel 1(b). Proses ini akan dilakukan sampai seluruh *plaintext* diproses. Setelah seluruh *plaintext* diproses, dilakukan proses penyelipan bilangan acak pada *cyphertext*.

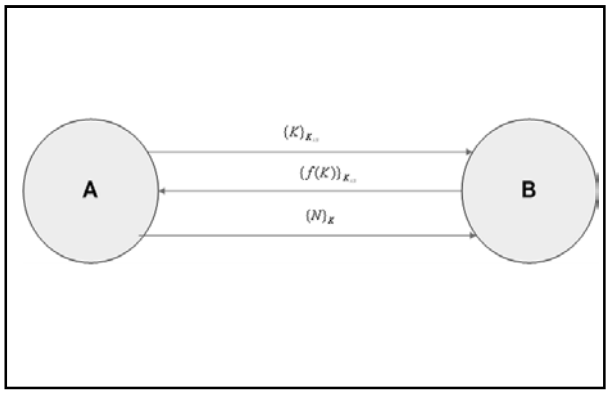
Proses dekripsi dilakukan dengan proses yang hampir sama dengan proses enkripsi seperti terlihat pada Gambar 2. Adapun perbedaannya terletak



Gambar 2 Diagram Alir Proses Dekripsi

hanya pada bagian awal proses. Dekripsi diawali dengan penelusuran letak bilangan acak pada *cyphertext*. Setelah posisi bilangan acak pada *cyphertext* ditemukan, maka dilakukan pengambilan *block* sepanjang 128 bit untuk kemudian dilakukan proses permutasi. Bilangan acak kemudian di-*XOR*-kan dengan hasil proses permutasi dan kemudian hasilnya mengalami proses *XOR*. Hasil proses *XOR* ini akan mengalami permutasi invers. Hal ini dilakukan berulang sampai seluruh *cyphertext* diproses, dan hasil terakhir berupa *plaintext* yang dikirim.

Untuk dapat meningkatkan keamanan dari pengiriman informasi digunakan kunci yang berbeda pada setiap pengiriman. Kunci yang digunakan pada sistem kriptografi ini dapat dikirim dengan menggunakan protokol seperti yang diperlihatkan Gambar 3.



Gambar 3 Protokol Kriptografi

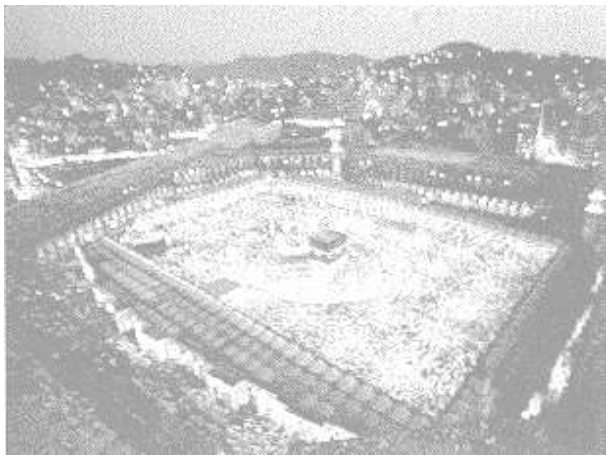
Pada protokol kriptografi yang ditunjukkan pada Gambar 3 diberikan beberapa asumsi diantaranya bahwa (1) A dan B telah menyepakati kunci bersama K_{ab} dan *one way function f* (Schneier, 1996; Menezes, et al, 1997) serta (2) A dan B saling mempercayai. Pada protokol tersebut terlihat bahwa A mengirim kunci *K* yang akan digunakan untuk mengenkripsi gambar kepada B. *K* dikirim setelah terlebih dahulu dienkripsi menggunakan K_{ab}. B kemudian akan mendekripsi pesan yang dikirimkan oleh A menggunakan K_{ab} untuk mendapatkan *K*. Setelah itu, B menerapkan *one way function f* pada *K* yang direpresentasikan dalam *f(K)* dan kemudian mengirimkannya kepada A. Setelah menerima *f(K)* yang dikirimkan oleh B, A menerapkan *f* pada *K* yang dimilikinya dan membandingkan antara *f(K)* yang dibuatnya dengan *f(K)* yang dikirimkan oleh B. Setelah keduanya diyakini sama, atau dengan kata lain B adalah pihak yang dituju A, maka A akan mengirimkan *file* gambar *N* yang telah dienkripsi menggunakan *K* kepada B. Proses enkripsi yang digunakan untuk mengenkripsi *N* akan mengikuti proses seperti yang ditunjukkan pada Gambar 1.

Keunggulan yang dibuat pada sistem kripto yang diusulkan ini dibandingkan dengan *VEA* adalah (1) metode untuk mengenkripsi tidak hanya menggunakan proses *EX-OR* dan (2) kunci yang dipakai pada setiap pengiriman gambar akan dibangun sesaat sebelum pengiriman gambar dan bersifat unik. Kedua hal ini disebutkan sebagai keunggulan karena kedua hal tersebut dapat meningkatkan kekuatan sistem kripto yang diusulkan ini. Adapun analisisnya dapat dilihat pada bagian Analisa.

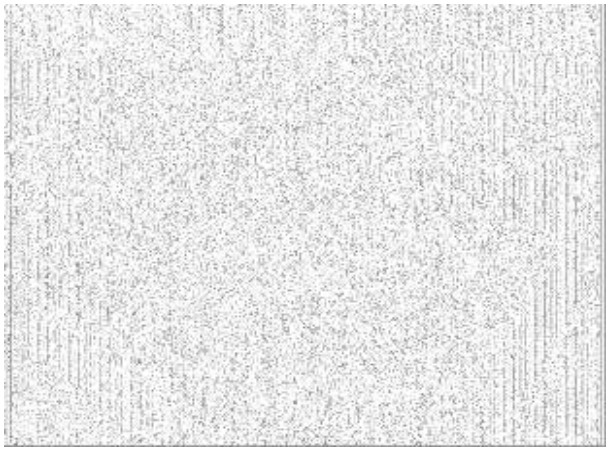
HASIL DAN PEMBAHASAN

Setelah diimplementasikan untuk gambar yang memiliki kedalaman warna 8 *bit per pixel* (*bpp*) dengan panjang kunci 256 *bit* atau 32 karakter, maka

diperoleh hasil seperti yang ditunjukkan pada Gambar 5.



Gambar 4 Gambar Asli



Gambar 5 Gambar Setelah Dienkripsi

Dari Gambar 4 dan 5 tampak perubahan gambar sebelum dan setelah dienkripsi dengan sistem kriptografi yang diusulkan. Dengan demikian, tampak jelas secara visual bahwa pola dari gambar asli tidak terlihat pada gambar hasil enkripsi.

Analisis Hasil

Pada sistem kriptografi yang diajukan digunakan proses *EX-OR* antara gambar dengan *pseudorandom number* yang dibangun dari kunci sebagai *seed*. Hal ini mengakibatkan kemungkinan untuk memecahkan *cyphertext* menjadi semakin kecil, karena kemungkinan untuk memecahkan kunci menjadi lebih kecil. Misalnya kunci adalah *K* yang dibangun dari 32 karakter atau 256 bit, maka kemungkinan untuk memecahkan kunci dengan *brute force attack* adalah sebesar $1/2^{256}$. Sementara itu, bila seseorang ingin memecahkan sistem kriptografi ini tanpa menggunakan kunci, maka ia harus memecahkan *pseudorandom number* yang digunakan dalam proses enkripsi. Bila dilakukan dengan *brute force attack*, maka berarti kemungkinan untuk memecahkannya adalah $1/2^{128}$. Jadi bila seseorang ingin melakukan *plaintext attack*. Maka ia tidak dapat langsung mendapatkan kuncinya atau *pseudo random number* yang digunakan, karena untuk mendapatkan *pseudo random number* yang digunakan perlu pengetahuan tentang kunci karena *pseudo random numbe*r yang digunakan disisipkan di dalam *cyphertext* pada posisi yang ditunjukkan oleh tiap bilangan pembentuk kunci. Dengan demikian *pseudo random number* tidak dapat diperoleh hanya dari *cyphertext* yang dikirimkan. Hal ini merupakan keunggulan dari sistem kriptografi yang diajukan dibandingkan dengan *VEA*. Dengan *VEA*, seseorang dapat segera memperoleh kunci setelah ia mengirimkan *plaintext* dan menerima *cyphertext*, sementara dengan sistem kriptografi yang diusulkan perlu dilakukan beberapa tahap untuk memecahkan kuncinya. Dari penjelasan di atas dapat dibuktikan bahwa sistem kriptografi yang diajukan mempunyai kekuatan yang lebih baik dibandingkan dengan *VEA* khususnya terhadap *plaintext attack.*

Menilik dari kecepatan eksekusinya, sistem kriptografi yang diusulkan ini memiliki kecepatan

yang lebih cepat dari *DES*, karena pada sistem ini tidak dilakukan proses *rounding*. Walaupun demikian, dibandingkan dengan kecepatan *VEA*, kecepatan eksekusi sistem kriptografi yang diajukan masih relatif lebih lambat, karena pada sistem ini dibutuhkan proses permutasi dan penyelipan bilangan *pseudo random number* pada *cyphertext*.

SIMPULAN

Pada makalah ini telah dibahas pengembangan sistem kriptografi, khususnya untuk gambar dan diharapkan mempunyai kinerja lebih baik dari *VEA*. Berdasarkan pada penjelasan sebelumnya, dapat disimpulkan bahwa sistem kriptografi yang diusulkan ini mempunyai keunggulan berupa kekuatan yang lebih baik dibandingkan dengan *VEA* dan kecepatan eksekusi yang lebih cepat dibandingkan dengan *DES*. Walaupun demikian, kecepatan eksekusi sistem kriptografi yang diusulkan masih lebih lambat dibandingkan dengan *VEA*.

Peluang pengembangan berikutnya adalah peningkatan kecepatan eksekusi dan kedalaman warna di atas 8 *bpp*.

RUJUKAN

Knuth, ED. 1998. *The Art of Computer Programming: Volume 2/ Seminumerical Algorithm*. ____: Addison Wesley Professional.

Menezes, A. and Van Oorschot, P. and Vanstone, S. 1997. *Handbook of Applied Cryptography*. Florida: CRC Press Inc.

Schneier, B. 1996. *Applied Cryptography*. _____: John Wiley and Sons Inc.

Shi, C and Bhargava, B. 1998a. An Efficient MPEG Video Encryption Algorithm. *Proceedings of the Seventeenth IEEE Symposium on Reliable Distributed*. Los Almitos, CA, USA : 381-386.

Shi, C and Bhargava, B. 1998b. A Fast MPEG Video Encryption Algorithm. *Proceeding of the Sixth ACM International Conference on Multimedia*. USA: 81-88.

Stinson, D. R. 1995. *Cryptography: Theory and Practice*. Florida: CRC Press, Inc.