ENKRIPSI GAMBAR DENGAN MENGGUNAKAN ALGORITMA ENHANCE 1-D CHAOTIC KEY BASED (ECKBA)

Fernando Manurung[1], Adiwijawa[2], Tjokorda Agung Budi Wirayuda[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Dengan seiring berjalannya kemajuan teknologi, banyak file multimedia berupa gambar yang harus diamankan dalam pendistribusiannya. Salah satunya adalah dengan teknik kriptografi dengan algoritma Enhance 1-D Chaotic Key Based (ECKBA). Dalam metode kriptografi, seseorang dapat menggunakan suatu kunci (password) dimana dia dapat mengubah suatu data asli (plaintext) ke dalam bentuk yang tidak dapat dibaca (ciphertext) dan mengembalikan ciphertext kembali ke plaintext. Dalam tugas akhir ini dibuat suatu aplikasi dengan menggunakan Matlab 7.1 dan menganalisis perbandingan antara ECKBA murni dengan ECKBA yang telah mengalami suatu proses preposesing. Parameter yang dibandingkan adalah nilai avalanche effect, kecepatan proses enkripsi dan dekripsi, besar file sesudah dienkripsi dan didekripsi, dan tingkat gangguan yang dihasilkan

Kata Kunci : gambar, Enhance 1-D Chaotic Key Based Algorithm (ECKBA), kriptograpfi.

Abstract

Due to the technology improvement, many multimedia files like picture have to be secured on its distribution. One of the techniques to secure the data is to encrypt them with cryptographic algorithm such as Enhance 1-D Chaotic Key Based (ECKBA). In cryptography method, somebody can use a key (password) where can change the original data (plaintext) into a form which can't be read (ciphertext), and change the ciphertext into plaintext. In this Final Task is made the implementation by using Matlab 7.1 and analysis the comparison between ECKBA and ECKBA with a preprocessing. The parameter that will be compared to are avalanche effect, the speed of encryption and decryption, the size of files after encryption and decryption, and noising level.

Keywords : picture, Enhance 1-D Chaotic Key Based Algorithm (ECKBA), kriptograpfi.

1. Pendahuluan

1.1 Latar Belakang

Gambar adalah suatu media yang dapat kita gunakan untuk mengabadikan suatu kejadian yang sangat penting atau berkesan dalam kehidupan kita. Dengan adanya gambar tersebut kita dapat mengenang kejadian-kejadian yang telah belangsung. Selain itu dengan adanya gambar kita dapat melihat objek-objek yang ada di dunia ini secara tidak langsung tanpa harus ke tempat objek tersebut.

Gambar juga dapat kita gunakan untuk berbagi pengalaman kita dalam bentuk objek gambar. Namun, gambar-gambar yang sangat berkesan atau lucu bagi kita tersebut terkadang sangat memalukan sekali jika dilihat oleh orang lain dan jika kita hapus sangat sayang sekali. Bukan hanya itu saja, pada saat ini banyak juga objek-objek yang diabadikan lewat gambar namun tidak boleh dilihat oleh orang lain seperti gambar proses melahirkan yang sedang marak saat ini, gambar letak kekuatan tentara pada saat perang, dan sebagainya.

Dengan adanya permasalahan di atas, maka Tugas Akhir ini berusaha untuk melindungi kerahasian yang ada pada suatu gambar, dengan melakukan enskripsi pada pada gambar tersebut. Enskripsi ini akan menyamarkan suatu gambar yang ada tanpa mengurangi kualitas yang ada pada gambar tersebut.

Banyak algoritma enskripsi yang telah dikembangkan antara lain: RC6, MRC6, Rijndael, RSA, RIPEMB128, RIPEMB160, Permutasi dan lain-lain. Pada tugas akhir ini akan digunakan metoda ECKBA (E*nhance 1-D Chaotic Key Based Algorithm*) yaitu metoda enkripsi yang berdasarkan atas prinsip chaos. Tugas Akhir ini, akan diimplementasikan dengan menggunakan Matlab sebagai media enskripsi dan deskripsi gambar tersebut.

1.2 Perumusan Masalah

Enhance 1-D Chaotic Key Based Algotihm (ECKBA) merupakan algoritma kriptografi kunci simetri. Permasalahan yang dijadikan objek penelitian dan pengembangan tugas akhir ini adalah:

1 Bagaimana mengamankan data berupa gambar dengan menggunakan *Enhance 1-D Chaotic Key Based Algotihm (ECKBA)* murni dan ECKBA dengan suatu proses preposesing.

2 Mengetahui bagaimana performansi algoritma ini dalam mengenkripsi data gambar berdasarkan parameter waktu enkripsi/dekripsi, *avalanche effect*, besar file input dan output, tingkat PSNR, serta tingkat ketahanan enkripsi gambar(*robustness*).

1.3 Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah :

1. Mengimplementasikan algoritma untuk mengenskripsi gambar dengan algoritma *Enhance 1-D Chaotic Key Based* (ECKBA) dalam sebuah aplikasi.
2. Menganalisis performansi (*avalanche effect*, kecepatan, besar file, dan tingkat PSNR, dan *robustness*) algoritma kriptografi ECKBA.

1.4 Batasan Masalah

Batasan masalah dalam tugas akhir ini adalah:

1. File masukkan yang digunakan adalah file image dengan format windows bitmap (*.bmp) dengan resolusi 128x128 pixel dengan kedalaman warna 8 bit grayscale.
2. Metode enskripsi yang digunakan adalah metode ECKBA.
3. Input dari sistem berupa gambar dan output berupa gambar hasil enskripsi.

1.5 Metodologi Penyelesaian Masalah

Metodologi yang digunakan untuk menyelesaikan masalah dalam Tugas Akhir ini adalah:

1. Studi Literatur
   Studi literatur dari beberapa buku, jurnal, artikel yang membahas tentang citra, kriptografi, algoritma ECKBA dan karakteristiknya serta pembuatan aplikasi dengan menggunakan Mathlab.
3. Perancangan Sistem
   Merancang pemecahan masalah berdasarkan hasil analisis yang didokumentasikan dalam suatu spesifikasi dengan menggunakan metode pengembangan perangkat lunak.
4. Implementasi
   Pembuatan aplikasi dengan menggunakan Matlab.
5. Pengujian
   Pengujian dilakukan dengan melakukan enskripsi pada beberapa gambar dengan kedua metode tersebut dengan berbagai ukuran gambar yang berbeda.
6. Analisis
   Melakukan analisis dari hasil pengujian sehingga didapatkan kesimpulan efektivitas pengunaan metode ECKBA.
7. Penyusunan Laporan
   Hasil penelitian akan disusun menjadi suatu laporan yang meliputi aspek-aspek dalam penelitian yaitu teori dan implementasinya.

1.6 Sistematika Penulisan

Struktur Pembahasan Tugas Akhir ini disusun sebagai berikut :

BAB I PENDAHULUAN

Menguraikan mengenai latar belakang dari sistem yang akan dibangun, perumusan masalah yang akan dianalisa, tujuan dari pembuatan sistem ini, pembatasan dari masalah yang terjadi, menentukan metodologi pemecahan serta sistematika penulisan.

BAB II LANDASAN TEORI

Merupakan keseluruhan teori yang mendukung pembuatan pengembangan sistem ini antara lain meliputi teori-teori tentang enkripsi (konsep dasar, metode enskripsi berbasis ECKBA) dan pembangunan aplikasi dengan menggunakan Mathlab.

BAB III ANALISA DAN PERANCANGAN SPK

Berisi tentang hasil analisa terhadap seluruh masalah dan kebutuhan perangkat lunak, juga membahas mengenai rancangan dari sistem.

BAB IV IMPLEMENTASI SISTEM

Merupakan implementasi dari perancangan sistem yang dibuat, dan dilanjutkan dengan analisa hasil pengujian aplikasi yang dibuat.

BAB V PENUTUP

Kesimpulan dari keseluruhan rangkaian pengerjaan dan penelitian pada Tugas Akhir yang dilakukan serta saran untuk perbaikan kedepannya.

5. Kesimpulan dan Saran

Pada bab ini, penulis mencoba menyimpulkan hasil dari seluruh uraian yang telah dijelaskan mulai dari tahap analisis sampai tahap implementasi dan memberikan saran-saran yang membangun.

5.1 Kesimpulan

1. Nilai ganguan (PSNR) yang dihasilkan setelah gambar dienkripsi sangat kecil (8 dB) sehingga gambar memiliki karakteristik yang sangat berbeda dari gambar aslinya.
2. Ukuran file gambar hasil enkripsi dan dekripsi sama karena tidak adanya perubahan nilai pixel.
3. Algoritma ECKBA kurang baik diimplementasikan untuk mengamankan data berupa gambar karena waktu rata-rata enkripsi dan dekripsi cukup lama (39 detik).
4. Nilai *avalanche effect* dengan *key* yang berbeda satu bit lebih baik (49.54 %) dari pada dengan key yang sama dan plantext yang beda satu bit karena metode ini bergantung pada nilai kunci.
5. Untuk penggunaan karakter kunci yang berbeda algoritma ECKBA memenuhi kriteria *robustness* karena manipulasi yang dilakukan terhadap kunci menghasilkan hasil enkripsi yang berbeda-beda sedangkan untuk penggunaan karakter kunci yang sama algoritma ECKBA tidak memenuhi kriteria *robustness* karena manipulasi yang dilakukan terhadap kunci menghasilkan hasil dekripsi yamg sama.
6. Enkripsi gambar dengan metode ECKBA tidak memenuhi kriteria robustness karena meskipun gambar dapat didekripsi gambar hasil dekripsi memiliki *noise* dimana besarnya *noise* sangat bergantung terhadap besarnya noise yang diberikan. Semakin besar *noise* yang diberikan maka gambar hasil dekripsi akan mengalami gangguan (*noise*) yang besar.

5.2 Saran

1. Berdasarkan nilai *key generator* untuk menghasilkan key, selain menggunakan padding dapat juga menggunakan fungsi hash
2. Dalam proses enkripsi dan dekripsi dapat menggunakan metode yang lain, contohnya:Chaos-Based Fededback Stream chipper (ECBFSC), DES, dan AES.
3. Algoritma ini dapat diimplementasikan dalam berbagai hal, seperti enkripsi/dekripsi data dan audio.
4. Untuk menganalisis ECKBA dari sisi keamanan (kriptanalisis).

Daftar Pustaka

[1] A. Mitra, Y. V Subba Rao and S. R. M. Prasanna. *A New Image Encryption Approach using Combinational Permutation Techniques*. IJCS,. Volume 1. Number 2. ISSN 1306-4428. 2006

[2] Away Gunaid. *The Shortcut of Matlab Programming.* Informatika Bandung. 2006

[3] Budiyono, Avon. 2004. *Enkripsi Data Kunci Simetris Dengan Algoritma Kriptografi LOK197*. Bandung: Institut Teknologi Bandung.

[4] Dharma, Eddy Muntina. *Diktat matakuliah Garfika Citra* , Bandung: STT Telkom, 2004

[5] Gonzales, Rafael C. *Digital Image Processing*, Addison-Wesley Publishing. Canada, 1987

[6] Ismaraditya Ryan, Tugas Akhir. *Preancangan Algoritma Kriptografi Berbasis Chaotic Kolmargorov Flow pada Field Programmable Gate Array (FPGA).* Jurusan Teknik Elektro STT Telkom Bandung

[7] J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997

[8] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law. *A Fast Image Encryption Scheme based on Chaotic Standard Map.* City University of Hong Kong

[9] Munir, R. Kriptografi. Informatika Bandung. 2006

[10] Socek, Daniel. Liy, Shujun. Spyros S. Magliverasz and Borko Furht, 2005. *Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption*, Center for Cryptology and Information Security and Department of Comp. Sci. and Engineering Florida Atlantic University, Department of Electronic and Information

[11] www.mathworks.com.

[12] Zuliansyah, M. *Diktat matakuliah Kriptograpi*. Bandung: STT Telkom, 2006