Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)
SAINTEKS 2019

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 886 - 889

Implementasi Algoritma SAFER K-64 untuk Mengamankan Citra Digital

Josfery Pardosi, Theresia Sri Melati Pasaribu, Nuraini

Prodi Teknik Informatika STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338, Medan, Indonesia

Abstrak

Saat ini pengiriman gambar melalui internet telah banyak digunakan, namun pengiriman gambar tersebut belumlah aman. Banyak pihak-pihak yang akan menyala gunakan gambar tersebut dengan menyadap, memanipulasi, atau menggunakan informasi tersebut untuk kepentingan-kepentingan pribadi. Ada banyak cara untuk mengamankannya dengan teknik kriptografi, salah satunya adalah SAFER K-64. Algoritma SAFER K-64 adalah *byte-oriented block enchipering algorithm* yang memiliki panjang blok 8*byte* (64bit) untuk *plain* dan *chiper*. Algoritma ini hanya menggunakan fungsi pergeseran, XOR, penambahan dan pengurangan bit dan fungsi matematika untuk memetahkan bit, tanpa melibatkan jaringan feistel. Algoritma ini juga terdapat transformasi linier yang tidak lazim (*unorthdox linier transform)* yang disebut dengan *Pseudo-Hadamard Transform* (PHT). Selain itu, pada pembuatan kunci untuk setiap ronde digunakan sebuah fungsi yang dapat menyebabkan kunci pada tiap ronde tidak lemah (*weak key*). Penelitian ini menguraikan tentang penerapan algoritma SAFER K-64 untuk mengoptimalkan keamanan citra digital berformat JPEG.

Kata Kunci: Kriptografi, SAFER K-64, Citra, JPEG.

1. PENDAHULUAN

Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpinan/diskrit nilai digital yang disebut *pixel/picture elements*. Dalam tinjauan matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi. Citra digital sangat banyak digunakan pada zaman modern ini terutama untuk mengabadikan moment. Penggunaan standar kompresi citra JPEG yang semakin meluas menjadikan isu keamanan pada standar ini harus diperhatikan. Standar JPEG tidak dilengkapi dengan standar layanan keamanan sehingga citra terkompres JPEG mudah diubah dan disdistribusikan baik secara legel maupun ilegel. *Secure* JPEG adalah sebuah *fraemwork* yang terbuka dan fleksibel berbagai metode keamanan telah dikembangkan untuk menghasilkan kualitas kemanan terbaik dengan adanya *secure* JPEG diharapkan mampu memberikan keamanan untuk citra JPEG yang ada sekarang[1].

Saat ini teknik kriptografi dapat diimplementasikan sebagai salah satu solusi yang cukup baik untuk digunakan dalam mengatasi masalah pengamanan data. Teknik kriptografi bekerja dengan mentransformasikan data asli menjadi sandi-sandi, sehingga pola dan makna data yang lama tidak lagi diketahui[2]. Teknik ini cukup ampuh untuk meminimalisir tindakan-tindakan yang dapat dilakukan oleh orang lain untuk menyalahgunakan data-data penting.

Secure And Fast Encryption Routine dengan *Key* panjang 64 bit (SAFER K-64) adalah algoritma yang pertama kali dikambangkan oleh J.L.Massey pada tahun 1991. SAFER K-64 merupakan algoritma *chiper block* yang membutuhkan 64 bit *plain* serta kunci 64 bit, algoritma ini terdiri dari 6 ronde iteratif dan ronde final namun bisa juga lebih dari 6 ronde, algoritma ini juga terbuat dari operasi byte sederhana makan dari itu sangat cocok untuk data dengan ukuran kecil[3]. SAFER K-64 juga membutuhkan 2-set sub kunci, kunci private 64 bit dibagi menjadi 8 block 8 bit. Kemudian setiap byte diputar ke kiri sebanyak 3bit dan hasilnya di simpulkan dengan konstanta putaran.

Tabel 1. Penelitian Terkait

No	Penulis	Judul	Kesimpulan
1	Syaiful Anwar, Indra Nugroho dan Asep Ahmadi	Implementasi Algoritma Kriptografi dengan Enkripsi Shift Vegenere Cipher serta Checksum Menggunakan CRC32 pada Data Text [4]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa teknik kriptografi dapat membatasi akses orang lain yang tidak berhak atas pesan atau data rahasia
2	Maulisa Oktiana, Khairul Munadi, dan Fitri Arnia	Metode Keamanan pada Citra JPEG-Ikhtisar [5]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa ada beberapa pendekatan yang bekerja dengan baik dalam mengamankan citra digital yaitu pendekatan dengan teknik *scrambling*, DCT, sistem ETC, *dynamic encryption* untuk keamanan arsitektur JPEG dan *privacy preserving photo sharing*
3	Ade Setiawan	Algoritma SAFER K-64 dan Keamanannya [6]	Berdasarkan penelitian terdahulu dapat disimpulkan bahwa algoritma SAFER K-64 ini hanya menggunakan fungsi aritmatika seperti modulo, logaritma, dan eksponen serta operasi manipulasi bit seperti pergeseran, penjumlahan, Xor, dan pengurangan

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 886 - 889

2. METODOLOGI PENELITIAN

2.1. Kriptografi

Teknik kriptografi bekerja dengan mentransformasikan data jelas (*plain*) ke dalam bentuk data sandi (*cipher*) yang tidak dapat dikenali. *Cihper* inilah yang kemudian dikirim oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai dipenerima, *chiper* tersebut ditranformasikan kembali ke dalam bentuk *plain* agar dapat dikenali. Arti lain dari kriptografi adalah sebagai salah satu seni dan ilmu dalam mengamankan pesan. Pesan asli disebut dengan plain atau *clear*, proses penyandian (pengubahan data asli) disebut dengan istilah enkripsi dan hasilnya disebut dengan istilah *chiper*. Proses pengembalian *chiper* menjadi *plain* disebut dekripsi[2]. Prinsip yang harus dicapai dalam penerapan teknik kriptografi adalah *confusion* (pembingungan) dan *diffusion* (peleburan)[7],[8].

2.2. SAFER K-64

Algoritma ini merupakan *chiper* blok 64-bit, dan mengulangi enam putaran dengan ditambah tranformasi output. SAFER K-64 di rancang oleh Massey sebagai anggota pertama dari keluarga yang aman dari *chiper* blok. SAFER K-64 adalah chiper *interated* dimana enkripsi dilakukan dengan menerapkan transformasi yang sama berulang kali untuk putaran r, kemudian menerapkan output transformasi, r = 6 atau lebih bila diinginkan keamanan yang lebih besar. Setiap putaran menggunakan dua subyek 8 byte (64 bit) yang ditentukan oleh kunci penjadwalan dari kunci rahasia 8 byte yang di pilih. Transformasi output menggunakan subyek 8 byte lain yang ditentukan oleh jadwal kunci. Salah satu fitur yang tidak biasa dari SAFER K-64 yaitu, berbeda dengan chiper blok *iterated* yang diusulkan dan memiliki enkripsi dan dekripsi yang sedikit berbeda[3]. Variasi algoritma SAFER disebut dengan algoritma SAFER SK. SK di sini berarti *Strengthened Key Schedule* (penjadwalan kunci yang diperkuat) dengan membuat fungsi penjadwalan kunci yang lebih baik. Versi lainnya seperti SAFER K-128, SAFER SK-64, SAFER SK-128, SAFER+, SAFER++[6],[9].

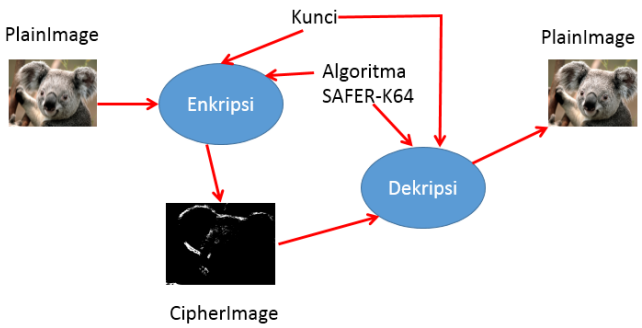
2.3 Citra Digital

Citra Digital adalah citra f(x,y) dimana dilakukan diskritisasi koordinat sampling/spasial dan diskritisasi tingakat kwantisasi (keabuan/kecemerlangannya). Citra digital merupakan fungsi intensitas cahaya f(x,y), dimana harga x dan harga y adalah koordinat spasial. Harga fungsi tersebut disetiap titik (x,y) merupakan tingkat kecemerlangan citra pada titik tersebut. Citra digital merupakan salah satu jenis data yang digunakan dalam berkomunikasi baik secara langsung atau media seperti internet dan pesan *chatting*. Namun seiring berkembangnya teknologi banyak pihak-pihak yang menyalagunakan data gambar tersebut dengan menyadap, memanipulasi, atau menggunakan informasi tersebut untuk kepentingan pribadi[1],[4],[5].

3. ANALISA DAN PEMBAHASAN

3.1 Analisa

Pengamanan citra digital berdasarkan teknik kriptografi menjadi salah satu upaya yang dapat digunakan untuk menjaga kerahasiaan data dari tindakan penyalahgunaan oleh pihak-pihak yang tidak bertanggungjawab. Teknik kriptografi dapat diterapkan dengan memanfaatkan salah satu algoritma kriptografi yang ada, salah satunya adalah algoritma SAFER K-64. Citra digital yang dijadikan sebagai contoh implementasi dalam penelitian ini adalah citra digital berformat JPEG, karena jenis ini umumnya banyak digunakan dalam berkomunikasi. Nilai-nilai *pixel* dari citra asli akan ditransformasikan menjadi nilai desimal terlebih dahulu, kemudian nilai-nilai desimal ini menjadi input proses enkripsi maupun dekripsi berdasarkan algoritma SAFER K-64 sehingga dihasilkan *cipherimage* dan sebaliknya. *Cipherimage* yang dihasilkan sebagai hasil akhir dari proses enkripsi tentu tidak lagi memperlihatkan pola citra asli. Kunci yang digunakan dalam proses enkripsi akan menambah kerumitan bagi orang lain untuk melakukan proses dekripsi kecuali pihak penerima yang sah.



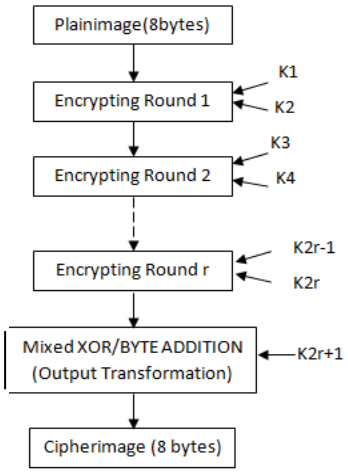
Gambar 1. Konsep Pengamanan Citra Dgital Berdasaran Algoritma SAFER K-64

3.2 Pembahasan

Algoritma enkripsi SAFER terdiri dari r putaran transformasi identik yang diterapkan di urutan ke plain, diikuti oleh transformasi keluaran, untuk menghasilkan final chiper. Rekomendasi kami adalah menggunakan r = 6. Setiap putaran dikontrol oleh dua subyek 8 byte dan transformasi output dikendalikan oleh satu subyek 8 byte. Ronde yang berjumlah r

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 886 - 889

akan dibangkitkan sebanyak 2r+1 buah kunci yang akan dibahas. Panjang kunci masukan *user* biasanya 8 byte. Jumlah semua plain, chiper dan sub kunci yang terlibat pada setiap proses enkripsi adalah sama yaitu 8 byte (64 bit).



Gambar 2. Proses Enkripsi Berdasarkan Algoritma SAFER

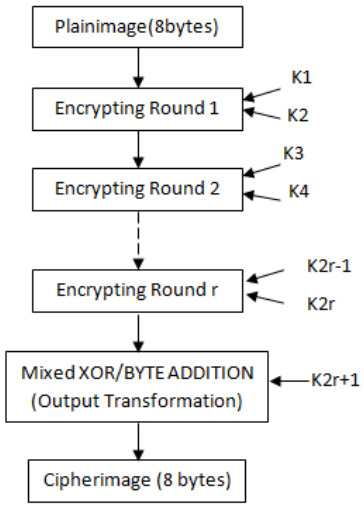
3.2.1 Fungsi Enkripsi

Fungsi Enkripsi pada algoritma SAFER pertama kali akan menggunakan operasi Xor, add. Memasuki proses transformasi Mixed Xor/*byte operation and addition*. Operasi Xor adalah ekuivalen dengan operasi penjumlahan bit bermodulo dua. Contohnya adalah :
0 Xor 2 = (0+2) mod 3 = 1
1 Xor 2 = (1+2) mod 3 = 0
0 Xor 0 = (0+0) mod 3 = 0

Operasi add adalah operasi penjumlahan byte dengan modulo 256. Perlu diperhatikan bahwa representasi byte di sini adalah bentuk integer. Yang berarti nilainya ada pada wilayah 0 hingga 28 = 255. Itulah sebabnya mengapa penjumlahannya modulo dengan 256. Contohnya adalah:
250 add 110 = (250+116) mod 256 = 110
110 add 25 = (11+25) mod 256 = 36

3.2.2 Algoritma Dekripsi dari SAFER

Algoritma dekripsi pada SAFER adalah kebalikan dari algoritma enkripsi, image ini lalu mengalami input transformasi dalam hal ini, ada pada *byte* ke-1,4,5,8 mengalami *substraction*, dan sisahnya mengalami operasi XOR. Operasi substraction ini adalah operasi pengurangan integer dari byte dan akan ditambah 256 jika nilainya minus.



Gambar 3. Proses Dekripsi Chipertext Berdasarkan Algoritma SAFER

4 KESIMPULAN

Kesimpulan yang didapat dari studi implementasi algoritma SAFER K-64 untuk mengamankan citra digital adalah algoritma SAFER K-64 adalah algoritma *blok chiper* dengan panjang blok 64 bit dan panjang kunci 64 bit. Peningkatan

ISBN: 978-602-52720-1-1
Januari 2019
Hal: 886 - 889

keamanan algoritma SAFER dapat dilakukan dengan menambah jumlah ronde enkripsi dan juga dengan mendesain penjadwalan kunci yang baru.

REFERENCES

[1] A. A. Nurcahyani and R. Saptono, "Identifikasi Kualitas Beras dengan Citra Digital," *Sci. J. Informatics*, vol. 2, no. 1, pp. 63–72, 2016.
[2] H. Inggiantowi and K. K. Android, "Studi Implementasi Algoritma Block Cipher pada Platform Android."
[3] J. L. Massey, "SAFER K-64 : A Byte . Oriented Block-Ciphering Algorithm."
[4] S. Anwar, I. Nugroho, and A. Ahmadi, "Implementasi Algoritma Kriptografi dengan Enkripsi Shift Vegenere Cipher serta Checksum Menggunakan CRC32 pada Data Text," *J. Sist. Inf.*, vol. 2, no. 1, pp. 51–58, 2015.
[5] M. Oktiana, K. Munadi, and F. Arnia, "Metode Keamanan pada Citra JPEG-Ikhtisar," in *Seminar Nasional dan Expo Teknik Elektro*, 2015, pp. 38–44.
[6] A. Setiawan, "Algoritma SAFER K-64 dan Keamanannya," 2009.
[7] T. Zebua, "Encoding the Record Database of Computer Based Test Exam Based on Spritz Algorithm," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 9, no. 1, p. 52-62, 2018
[8] N. E. S. Doc, K. U. L. Wp, and J. N. Jr, "Impossible Differential Attacks on Reduced-Round," pp. 1–18, 2003.
[9] L. R. Knudsen, "A Key-schedule Weakness in SAFER K-64," pp. 274–286, 1995.