PENGAMANAN PELAPORAN DATA HIV / AIDS DI RUMAH SAKIT DAERAH dr. RADEN SOEDJATI PURWODADI MENGGUNAKAN CHAOTIC STREAM CIPHER DAN STEGANOGRAFI END OF FILE

Bayu Wicaksono[1], Umi Rosyidah, S.Kom. M.T[2]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Nakula 1 No. 5-11, Semarang, 50131, Telp: (024) 3517261, Fax : (024) 325 0165
E-mail :pierrotbolnez@gmail.com[1],burosyidah.umi@gmail.com[2]

Abstrak

Sistem pelaporan hasil temuan kasus baru HIV / AIDS di RSD dr. R. Soedjati Purwodadi masih dikerjakan secara manual, sekalipun laporan tersebut bersifat sangat rahasia namun pengamanannya masih sangat sederhana. Sehingga perlu direncanakan sistem pelaporan yang lebih terjamin tingkat kerahasiannya. Karena apabila pelaporan secara kualitatif yang berisi data lengkap dari penderita HIV / AIDS jatuh ke tangan yang salah / pihak yang tidak bertanggung jawab akan menimbulkan dampak psikososial bagi penderita HIV / AIDS yang bersangkutan dan keluarga penderita. Di mana dampak tersebut bisa menyangkut harga diri hingga karir penderita beserta keluarganya.Dengan menggunakan kombinasi metode kriptografichaotic stream cipherdan steganografi end of filepada data HIV / AIDS RSD dr. R. Soedjati, di mana chaotic stream cipher digunakan untuk menyandikan arsip sedangkan steganografi end of file digunakan untuk menyembunyikan keberadaan arsip di dalam media penampung. Melalui penelitian ini, didapatkan bahwa penggunaan kombinasi kriptografichaotic stream cipher dan steganografi end of fileberhasil mengamankan file data pelaporan HIV / AIDS di RSD dr. R. Soedjati dengan memberikan dua layer keamanan yang berfungsi dengan sangat baik. Setelah dilakukan lima kali percobaan dengan media penampung yang memiliki format berbeda, didapatkan keberhasilan sebesar 100% baik dalam proses enkripsi, encoding, decoding, dan dekripsi.

Kata kunci :*Data HIV / AIDS, kriptografi, chaotic stream cipher, , steganografi, end of file.*

Abstract

Results reporting system of HIV / AIDS new cases in RSD dr. R. Soedjati Purwodadi still done manually, even if the report is strictly confidential, but security was still very minimum. So, a more secure reporting system needs to be planned to guarantee the confidentiality level. Because if the qualitative reporting that contains the complete data of people living with HIV / AIDS fall into the wrong hands / parties who are not responsible, it will cause a psychosocial impact for HIV / AIDS sufferers and families concerned. Which these impacts could involve up to patients and their families career and esteem.Therefore, by using a methods combination of chaotic stream cipher cryptography and end of file steganography to provide two layers of security for HIV / AIDS data in RSD dr. R. Soedjati, where chaotic stream cipher used to encrypt the archives while end of file steganography is used to conceal the existence of the archive in the media container to deceive those who do not have authorization to access the archive, which the expected result is beside the contents of the archive can not be understood, the archives are also hidden as if the file does not exist. Through this study, successfully showed that the combined use of chaotic stream cipher cryptography and end of file steganography was managed to secure the data file reporting of HIV / AIDS in RSD dr. R. Soedjati by providing two layers of security that work very well. And after five trials with the media container that has a different format, obtained 100% success both in the encryption, encoding, decoding, and decryption process.

Keyword :*HIV / AIDS data, cryptography, chaotic stream cipher , steganography, end of file.*

1. PENDAHULUAN

Permasalahan HIV / AIDS sampai saat ini masih menjadi fenomena gunung esdi berbagai wilayah di Indonesia. Penderita HIV / AIDS di Indonesia sendiri masih distigmakan sebagai suatukeadaan yang belum bisa diterima oleh masyarakat secara luas. Maka dari itu pemerintah mengambil kebijakan penanggulangan HIV / AIDS secara terstruktur dan kelembagaan yang bekerja di berbagai bidang maupun sektor.

Upaya pemerintah dalam menurunkan angka kasus HIV / AIDS masih dianggap belum memuaskan,karena dari berbagai temuan kasus baru dan pelaporan dari waktu ke waktu belum menunjukkan penurunan kasus secara signifikan.
Untuk mencapai hasil yang diharapkan, diperlukan suatu langkah yang sinergis dan terorganisir yang didukung pelaporan akurat dengan berbagai sifat, baik itu yang bersifat sangat rahasia maupun terbuka.

Sistem pelaporan hasil temuan kasus baru HIV / AIDS di RSD dr. R. Soedjati Purwodadi masih dikerjakan secara manual, sekalipun laporan tersebut bersifat sangat rahasia. Sehingga perlu direncanakan sistem pelaporan yang lebih terjamin tingkat kerahasiannya. Karena apabila pelaporan secara kualitatif jatuh ke tangan yang salah / pihak yang tidak bertanggung jawab akan menimbulkan dampak psikososial bagi penderita HIV / AIDS yang bersangkutan.

Berdasar pada analisa dari masalah tersebut, maka penulis mengajukan judul penelitian "Pengamanan Pelaporan Data HIV / AIDS Di Rumah Sakit Daerah dr. Raden Soedjati Purwodadi Menggunakan Chaotic Stream Cipher Dan Steganografi End of file" sebagai bahan pertimbangan dalam proses pengamanan pelaporan data HIV / AIDS.

2. TINJAUAN PUSTAKA

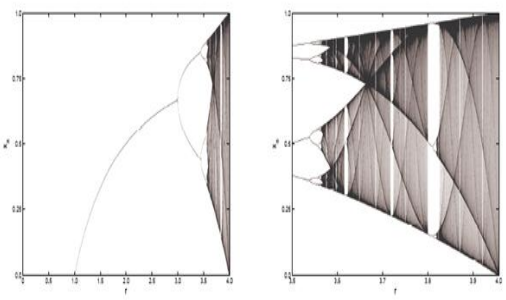
2.1 Teori Chaos

Teori chaos adalah teori yang menggambarkan perilaku sistem dinamis nirlanjar yang menunjukan fenomena yang kacau. Salah satu teori sistem chaos adalah sangat peka terhadap nilai awal. Hal ini menunjukan hasil yang sangat kacau jika nilai awal berbeda sedikit saja. Map dari suatu nilai tertentu yang polanya sangat sensitif terhadap perubahan disebut *Chaotic Map*. Ada banyak chaotic map yang telah ditemukan, salah satunya adalah *Logistic Map*.

Logistic Map merupakan salah satu fungsi chaos sederhana di dalam ekologi yang digunakan untuk mensimulasikan pertumbuhan populasi spesies. *Logistic Map* juga merupakan satu dimensi yang telah digunakan secara luas, yang didefinisikan sebagai berikut :

$$X_{i+1} = r\ X_i (1 - X_i)(1)$$

Dari persamaan di atas, X adalah populasi spesies pada interval waktu yang ditentukan dengan X_0 adalah nilai awal iterasi. Daerah asal X adalah dari 0 sampai 1, yang dalam hal ini 1 menyatakan populasi maksimum dan yang 0 menyatakan kepunahan, sedangkan $0 \leq r \leq 4$. Konstanta *r* menyatakan laju pertumbuhan. Konstanta *r* juga menyatakan bagian nirjalar dari persamaan. Ketika *r* meningkat, maka sistem juga naik.



Gambar 1. Diagram *bifurcation* untuk persamaan logistik

Gambar 1. di atas memperlihatkan kelakuan fungsi yang dalam hal ini sumbu-*x* menyatakan nilai *r* sedangkan sumbu-*y* menyatakan status sistem, yaitu nilai x. Bila 0 <*r*< 1, nilai awal berapapun akan menghasilkan kepunahan. Bila 1 <*r*< 3, fungsi konvergen ke sebuah nilai *(fixed-point)*, yaitu nilai *r* yang menghasilkan sistem yang mempunyai periode satu siklus. Ketika *r* = 3, kurva fungsi terpecah menjadi dua *(bifurcation)* menghasilkan dua nilai populasi yang berbeda, yang berarti nilai X secara periodik berosilasi dari status tinggi ke status rendah. Periode sistem pada nilai *r* ini adalah dua. Ketika *r* meningkat lagi, kurva fungsi terpecah lagi menjadi empat, yang berarti nilai-niklai X yang dihasilkan berosilasi di antara 4 nilai. Periode sistem pada nilai *r* ini adalah empat.

Demikian seterusnya *bifurcation* menjadi lebih cepat lagi dengan meningkatnya nilai *r* sampai tiba pada suatu nilai *r* tertentu sifat chaos pun muncul. Pada titik ini tidak mungkin lagi memprediksi kelakuan sistem. Kita dapat melihat bahwa ketika *r*> 3.75 sistem mulai melaju dengan cepat menuju area chaos (gambar yang diasir). Akhirnya, ketika *r* = 4, iterasi bergantung sepenuhnya terhadap nilai awal atau X_0 dan nilai-nilai yang dihasilkan muncul acak meskipun sistem ini deterministik. Nilai-nilai chaos yang dihasilkan akan berada di dalam rentang yang lengkap anatara 0 dan 1.

Fungsi *Chaos* yaitu menggunakan *Logistic Map* banyak digunakan pada kriptografi. Karena *Logistic Map* mempunyai kesensitifan pada nilai awal sehingga menghasilkan kekacauan. Kekacauan tersebut diterapkan pada kunci pada kriptografi.Sehingga cocok untuk dikembangkan di masa depan.

2.2 Stream Cipher

Aliran kode *(cihper stream)* mengenkripsi teks-asli menjadi teks-kode bit per bit (1 bit setiap kali transformasi). Pertama kali diperkenalkan oleh Vernam melalui algoritma yang dikenal dengan nama kode Vernam. Cipher aliran merupakan versi lain dari *one-time-pad*.

Satu-satunya algoritma kriptografi yang sempurna aman dan tidak dapat dipecahkan adalah one the pad (secara matematis Shannon telah membuktikan bahwa OTP tidak dapat dipecahkan). OTP ditemukan pada tahun 1917 oleh Vernam dan Major Joseph Mauborge. *One Time Pad* (*pad* = kertas bloknot) adalah kertas yang berisi deretan karakter-karakter kunci yang berisi huruf-huruf yang tersusun acak. Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci one-time pad :

$$C_i = (P_i + K_i) \bmod 26 \quad (2)$$

Setelah pengirim mengenkripsikan pesan dengan kata kunci, ia menghancurkan kunci tersebut (oleh karena itu disebut sekali pakai atau *one-time*). Penerima pesan menggunakan kunci yang sama untuk mengdekripsikan karakter-karakter

cipherteks menjadi karakter-karakter plainteks dengan persamaan:

$$P_i = (C_i - K_i) \bmod 26 \quad (3)$$

Shanon membuktikan apabila sandi *one time pad* diterapkan secara benar maka akan mencapai rahasia sempurna, (Shannon, 1949). Sebuah sandi disebutkan demikian bila pasangan teks asli dan teks sandi tidak memiliki hubungan statistik sehingga sulit bagi penyerang untuk melakukan analisis sandi atau analisis statistik.

Stream Cipher yang terdahulu secara umum dapat diserang, akan tetapi untuk desain *Stream Cipher* yang baru sangatlah sulit. Perlu banyak tambahan teknik dan literatur yang perlu dikembangkan untuk kriptanalisis. Sehingga perlu adanya pembaharuan untuk menyerang sesuatu yang juga baru didesain.

2.3 Metode Steganografi *End of file* (EOF)

Teknik yang digunakan pada *steganografi*beragam tetapi secara umum teknik inimenggunakan *redundant bits* sebagai tempatmenyembunyikan pesan pada saat dilakukankompresi data, dan kemudian menggunakankelemahan indera manusia yang tidak sensitivesehingga pesan tersebut tidak ada perbedaan yangterlihat atau yang terdengar. Teknik EOF atau *end of file*merupakan salah satu teknik yang digunakandalam steganografi. Teknik ini digunakan dengancara menambahkan data atau pesan rahasia padaakhir *file*. Teknik ini dapat digunakan untukmenambahkan data yang ukurannya sesuai dengankebutuhan. Perhitungan kasar ukuran *file* yang telahdisisipkan data sama dengan ukuran *file* sebelumdisisipkan data ditambah ukuran data rahasia yangtelah diubah menjadi *encoding file*.

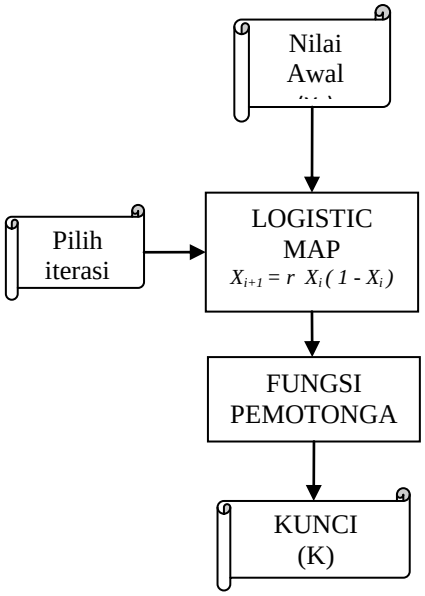
Steganografi dengan metode EOF banyak dipakai terutama dalam pembuatan instalasi (setup) dan SFX (Self Extractor). Setup maupun SFX (yang biasanya terdapat sebagai fitur archiver semacam WinZIP, WinRar dan 7Zip) menggunakan metode ini dengan meletakkan data di akhir sebuah file EXE. Bila file EXE tadi dijalankan, dia akan membaca data di akhir dirinya dan meng-copy-nya ke folder yang ditentukan.

3. PEMBAHASAN

Metode yang diusulkan meliputi pembangkitan kunci, penerapan kunci pada Stream Cipher, dan penerapan metode *end of file* pada steganografi. Pada kriptografi, ada beberapa komponen terpenting yang harus ada yaitu plainteks, kunci, dan cipherteks. Ketiga komponen tersebut adalah bahan utama untuk melakukan proses enkripsi dan dekripsi.Sedangkan padametode *end of file*terdapat komponen penting yang harus ada untuk bisa melakukan *encoding* dan *decoding*, yaitu *covertext,hiddentext, data header, dan flag.*

3.1 Pembangkitan Kunci Chaos

Untuk membangkitkan kunci yang acak, penulis menggunakan teori chaos yang mempunyai properti yang berharga bagi kriptografi. Dalam teori chaos terdapat rumus *Logistic Map* sebagai pembangkit kunci acak yang akan menghasilkan iterasi berdasarkan nilai awal. Di bawah ini adalah desain untuk pembangkit kunci dalam penelitian ini :



Gambar 2. Proses urutan pembangkit kunci

Pembangkit kunci dengan *Logistic Map* yaitu tergantung pada nilai awal (X_0) yang dimasukan. Dengan menerapkan rumus :

$$X_{i+1} = r\ X_i (1 - X_i) \quad (1)$$

X_i : iterasi ke-i
r : konstanta

konstanta *r* adalah 4 untuk memenuhi ketergantungan sistem terhadap nilai awal (X_0) yang sebelumnya telah dimasukan. Pada penelitian ini, dapat pemilihan nomor iterasi tertentu dapat dijadikan deretan awal dalam pembangkitan kunci. Lalu iterasi pertama (X_1) dihasilkan dan berhenti sebanyak kunci yang akan dibangkitkan (Xn). Sehingga akan dihasilkan deretan nilai *Chaos* yaitu X_1, X_2, X_3, X_4, X_5,...Xn.

Setelah deretan nilai *Chaos* dihasilkan, selanjutnya akan dilakukan proses pemotongan untuk mendapatkan nilai integer. Cara untuk mendapatkan nilai integer adalah dengan mengambil sebanyak tiga angka terbelakang.

Dari masing-msing deretan nilai Chaos yang dihasilkan dan sudah mengalami proses pemotongan untuk mendapatkan nilai integer yaitu tiga angka terbelakang maka kunci sudah terbentuk. Yaitu dari X_1, X_2, X_3, X_4, X_5,...Xn setelah mengalami proses pemotongan menjadi K_1, K_2, K_3, K_4, K_5,...Kn.

3.2 Penerapan kunci Chaos pada Stream Cipher

Stream Cipher mengenkripsi dengan menambahkan plainteks dengan kunci dan dilanjutkan dengan modulo 256. Perhitungan integer berdasarkan nomor ASCII.

Plainteks : { P_1, P_2, P_3, P_4, ..., Pn }
Kunci : { K_1, K_2, K_3, K_4, ..., Kn}
_____mod 256_____(+)
Cipherteks: { C_1, C_2, C_3, C_4, ..., Cn }

Setelah deretan desimal dari cipherteks terbentuk lalu diubah menjadi deretan hexadesimal.

Sebelum melakukan dekripsi, pada cipherteks ditambah dengan 256 sejumlah kali sampai lebih besar dari elemen pad atau kunci, maka cipherteks dapat dikurangi oleh nilai dari deretan kunci yang sudah dibangkitkan sebelumnya.

Untuk menciptakan dari deretan cipherteks asli ke yang baru akan dilakukan proses dan kondisi sebagai berikut :

$$C_{nb} = (256 \text{ X } n) + C_{nl} \quad (6)$$

lalu ambil nilai n terkecil yang memenuhi kondisi ($C_{nb} \geq K_n$).

n : konstanta
C_{nb}: Cipherteks baru
C_{nl} : Cipherteks lama

Sehingga dari deretan cipherteks lama $\{C_{nl1}, C_{nl2}, C_{nl3}, C_{nl4}, C_{nl5}, ..., C_{nl}n\}$

menjadi deretan cipherteks baru
$\{C_{nb1}, C_{nb2}, C_{nb3}, C_{nb4}, C_{nb5}, ..., C_{nb}n\}$.

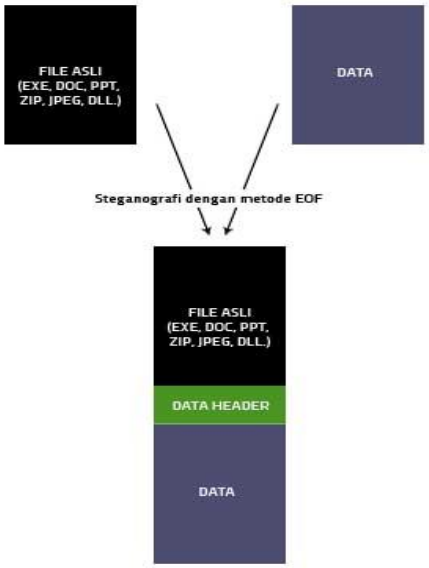
Cipherteks:{C_{nb1},C_{nb2},C_{nb3},C_{nb4},...,C_{nb}n}

Kunci : { K_1, K_2, K_3, K_4, ..., Kn}
_____mod 256_____(+)
Plainteks : { P_1, P_2, P_3, P_4, ..., Pn }

Setelah deretan desimal dari plainteks terbentuk lalu diubah menjadi deretan plainteks string asli.

3.3 Penerapan metode Steganografi *End of file* (EOF)

Dengan metode EOF, secara umum media steganografi (file yang akan disisipi data) memiliki struktur seperti ini:

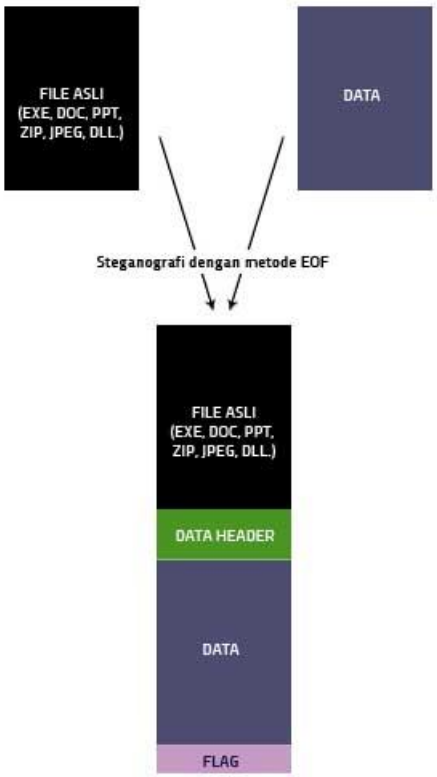


Gambar 3. Struktur Umum Steganografi Dengan Metode EOF

Setiap blok pada sebuah file dapat dibaca dengan menggunakan dua parameter, posisi awal dan panjang blok tersebut. Dengan struktur di atas, dapat dibaca posisi [DATA HEADER] yang isinya meliputi:

a. Posisi awal [DATA / Hiddentext] pada file
b. Panjang [DATA / Hiddentext] pada file

Untuk menentukan posisi dan panjang [DATA HEADER] itu sendiri, dapat dipakai looping yang mencari penanda (FLAG) sebagai penentu posisi awal [DATA HEADER] pada file media, mulai dari awal file. Namun cara ini akan menjadi tidak efisien dan menjadi lambat apabila file media [FILE ASLI / Covertext] berukuran sangat besar (misalnya 100MB).



Gambar 4. Penempatan FLAG

Karenanya, penanda [DATA HEADER] atau FLAG akan diletakkan di awal atau akhir file, di mana tidak ada looping yang digunakan untuk mencarinya. Pada beberapa file seperti EXE dan ZIP, penempatan FLAG di awal [FILE ASLI / Covertext] tidak akan menjadi masalah, namun untuk jenis file lain semisal JPG, BMP dan

DOC, penempatan FLAG di awal file akan merusak [FILE ASLI / Covertext] karena mengganggu isi [FILE ASLI / Covertext] dan merusak CRC file tersebut. Penulis akan menempatkannya di akhir file sehingga tidak membawa bencana meskipun digunakan berbagai jenis file. Ini juga sesuai dengan konsep EOF pada steganografi ini.

4. KESIMPULAN DAN SARAN

Dari hasil penelitian dan perancangan aplikasi pada penerapan *Chaotic Stream Cipher* danSteganografi *End of File* untuk pengamanan pelaporan data HIV / AIDS di Rumah Sakit Daerah dr. R. Soedjati Purwodadi ini, dapat diambil kesimpulan sebagai berikut :

1. Kombinasi *Chaotic Stream Cipher* Stganografi *End of File* menghasilkan sistem keamanan dua *layer* yang berfungsi dengan baik bagi pengamanan pelaporan data HIV / AIDS di RSD dr. R. Soedjati Purwodadi.
2. Layer keamanan pertama berupa file gambar memiliki fungsi untuk mengelabui pihak yang tidak terotorisasi, di mana file gambar merupakan tipe file yang paling sering diabaikan. Penggunaan steganografi *end of file* yang tidak menimbulkan perubahan fisik kepada file gambar juga mempersulit proses *steganalyst* untuk mendeteksi keberadaan pesan di dalam gambar.
3. Layer keamanan kedua berupa *Chaotic Stream Cipher* yang secara teknis tingkat keamanannya setara dengan*One Time Pad*(OTP) merupakan layer perlindungan terakhir yang sangat kuat terhadap serangan kriptanalis.
4. Teori *ChaosLogistic Map* membangkitkan kunci yang acak. Pada algoritma kriptografi, di dalam kunci pada umumnya banyak karakter yang digunakan sehingga terkesan panjang,di mana kunci yang panjang dan acak merupakan kunci yang baik dalam kriptografi.
5. File gambar stegotext yang mengalami perpindahan data melalui media penyimpanan eksternal, e-mail, dan social media dapat di *decode* dengan sempurna. Dan file *hiddentext* yang didapatkan bisa didekripsikan dengan sempurna.
6. File *stegotext*tidak mengalami kerusakan setelah dikompresi dengan menggunakan format .rar. File image masih tetap dapat didecode dengan sempurna.

Di bawah ini adalah beberapa saran yang perlu diketahui dan dimengerti untuk memaksimalkan hasil yang didapat :

1. Terdapat beberapa variasi yang bisa digunakan untuk memperkuatfungsi *logistic map* pada *Chaotic Stream Cipher* ini, yaitu melalui pemilihan iterasi, penambahan batasan digit nilai awal, dan pemilihan digit nilai awal yang berbeda.
2. Hindari penggunaan nilai awal 0.25, 0.5 dan 0.75, karena hasil iterasi yang dibangkitkan nilainya akan sama denganiterasi-iterasi berikutnya sehingga fungsikeamanan yang ingin dicapai melalui *logistic map* akan sia - sia.
3. Untuk penggunaan steganografi *End of File*, jika

sekiranya media penampung yang berupa file gambar dirasa kurang efisien, dapat diganti dengan media penampung lain. Namun, jika user ingin tetap menggunakan file gambar sebagai media penampung, metode algoritma steganografi lain yang *resistant*terhadap pengeditan gambar yang berpotensi merusak isi data dapat digunakan untuk menggantikan metode *End of File*.

4. Disarankan untuk tidak meakukan proses *editing* yang dapat mengubah posisi bit pada gambar, seperti *cropping*, *rotating*, *recoloring*, dan lain - lain, dikarenakan hal -hal yang secara langsung mengubah posisi bit - bit gambar dapat mengacaukan posisi pembacaan *data header* pada steganografi.

5. DAFTAR PUSTAKA

[1] Mina Mishra and Vijay H. Mankar, "Chaotic Encryption Scheme Using 1-D Chaotic Map," *Int. J. Communications, Network and System Sciences*, pp. 452-455, April 2011.

[2] Fengjian Wang, Yongping Zhang, and Tianjie Cao, "Research of chaotic block cipher algorithm based on Logistic map," *2009 Second International Conference on Intelligent Computation Technology and Automation*, pp. 678-681, 2009.

[3] P. Jhansi Rani and S.Durga Bhavani, "Symmetric Encryption using Logistic Map," *1st Int'I Conf. on Recent Advances in Information Technology I RAIT-20121*, 2012.

[4] Nicolas Friot, and Jacques M. Bahi Christophe Guyeux, "Chaotic iterations versus Spread-spectrum:chaos and stego security," pp. 1-10, January 2011.

[5] Catur Iswahyudi, Emy Setyaningsih, and Naniek Widyastuti, "PENGAMANAN KUNCI ENKRIPSI CITRA PADA ALGORITMA SUPER ENKRIPSI," *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III*, pp. 278-285, November 2012.

[7] Rinaldi Munir, *Kriptogafi*. Bandung, Indonesia: Informatika Bandung, 2006.

[9] Dony Ariyus, *PENGANTAR ILMU KRIPTOGRAFI Teori, Analisis, dan Implementasi*. Yogyakarta: C. V. ANDI OFFSET (Penerbit ANDI), 2008.

[11] Ervyn Yoga Indra K., "PENERAPAN TEORI CHAOS PADA KRIPTOGRAFI MENGGUNAKAN ALGORITMA STREAM CIPHER DAN ELECTRONIC CODE BOOK (ECB) UNTUK KEAMANAN PESAN TEKS," pp. 29 -31, August 2014.

[12] Rinaldi Munir, Bambang Riyanto , and Sarwono Sutikno , "Perancangan Algoritma Kriptografi Stream Cipher dengan Chaos," Bandung, 2005.

[13] Wasino, Tri Puji Rahayu, and Setiawan, "IMPLEMENTASI STEGANOGRAFI TEKNIK END OF FILE DENGAN ENKRIPSI RIJNDAEL," *Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012)*, pp. 150-157, March 2012.

[15] Eko Hari Rachmawanto, "TEKNIK KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA VERNAM CHIPER DAN STEGANOGRAFI DENGAN METODE END OF FILE (EOF)," p. 44, April 2010.