PENGAMANAN FILE GAMBAR MENGGUNAKAN FUNGSI ALGORITMA STEGANOGRAFI LSB DARI SERANGAN BRUTE FORCE

Kristin Daya Rohani Sianipar[1], Lia Cintia Purba[2], Septri Wanti Siahaan[3], Indra Gunawan[4],Sumarno[5]
[1,2,3,4,5]Program Studi Teknik Informatika
[1.2..3.4.5]STIKOM Tunas Bangsa Pematangsiantar
[1.2.3.4.5]Jl.Jend. Sudirman Blok A, No. 1,2 dan 3, Kota Pematangsiantar, Sumatera Utara
[1]kristinsianipar7@gmail.com, [2]liapurba99@gmail.com, [3]septriwanti26@gmail.com, [4]indra@amiktunasbangsa.ac.id, [5]sumarno@amiktunasbangsa.ac.id

Abstrak

Pada saat ini, kemajuan teknologi dibidang ilmu komputer dan telekomunikasi sangatlahberkembang dan maju dengan pesat. Pengamanan data merupakan hal yang sangat penting untuk menjagaisi datayang penting dari pihak-pihak yang dapat merugikan dengan cara merusak data-data penting dari pemilik data, salah satunya yaitu data gambar. Dengan meningkatkan keamanan data menggunakan kombinasi algoritma, dapat menjagakeamanan data lebih terjamin dari serangan-serangan yang dapat membahayakan isi dari data yang tersimpan. Kombinasi algoritma yangdigunakan untuk pengamanan data yaitu algoritma steganografi LSB. Jadi, dengan menggunakan kombinasi algoritma steganografi LSBtingkat pengamanan filegambar bisa lebih terjaga keaslian datanya dan lebih efisien.

Kata kunci : ***pengamanan data, algoritma steganografi LSB***

DOI: https://doi.org/10.29103/techsi.v10i1.606

Abstract

At this time, technological advances in the field of computer science and telecommunications are highly developed and developed rapidly. Data security is very important to maintain the important data content of the parties that can harm by destroying the important data from data owner, one of which is image data. By improving data security using a combination of algorithms, it can keep data security more secure than attacks that can harm the contents of data stored. The combination of algorithms used for data security is LSB steganography algorithm. So using the combination of steganography algotitma Lsb file security level of the image can be more awake its data authenticity and more efficient.
Keywords** : **data security, LSB steganography algorithm

I.PENDAHULUAN

A. Definisi Bruto Force

Brute Force adalah algoritma yang memecahkan masalah dengan sangat sederhana,langsung dan dengan cara yang jelas/lempang. Penyelesaian permasalahan kode cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter dan panjang kode tertentu tentunya dengan banyak sekali kombinasi kode. Algoritma brute force adalah algoritma yang lempang atau apa adanya. Pengguna hanya tingal mendefinisakan karakter set yang diinginkan dan berapa ukuran dari kodenya. Tiap kemungkinan kode akan digenerate oleh algoritma ini (Gunawan, 2016). Maka dengan menggunakan algoritma brute force pengguna dapat lebih efisien dalam memecahkan keamanan *file* gambar.

B. Definisi Steganografi

Steganografi (*steganography*) berasal dari bahasa yunani yaitu*steganos* yang memiliki arti tersembunyi dan *graphein* yang berarti menulis, sehingga jika disatukan, maka artinya adalah "menulis tulisan yang tersembunyi"[2]. Steganografi

DOI: https://doi.org/10.29103/techsi.v10i1.606

(steganography) adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima ,tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Aspek terpenting pada steganografi adalah tingkat keamanan penyembunyian informasinya yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi.

II. METODE PENELITIAN

A. Metode yang Dipakai Brute Force Attack

Brute Force attack adalah sebuah metode untuk menjebol kode rahasia (yaitu, mendekripsi sebuah teksyang telah terenkripsi) dengan mencoba semua kemungkinan kunci yang ada. Feasibility darisebuah brute force attack tergantung dari panjangnya cipher yang ingin dipecahkan , dan jumlah komputasi yangtersedia untuk penyerang. Salah satu contohnya bernama Cain's Brute Force Code Cracker mencoba semua kombinasi yang mungkin dari karakter yang telah didefinisikan sebelum atau set karakter yang kustom melawan sebuah kode yang telah terenkripsi di brute force dialog. Kuncinya adalah mencoba semua kemungkinan kode dengan formula seperti berikut. KS = L(m) + L(m+1) + L(m+2) + ... + L(M).

L = jumlah karakter yang kita ingin definsikan m = panjang minimum dari kunci M = panjang maksimal dari kunci. Contohnya saat kita ingin meretas sebuah Lan Manager paswords (LM) dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter, maka brute fore cracker harus mencoba KS = 26^1 + 26^2 + 26^3 + ... + 26^7 = 8353082582 kunci yang berbeda.

Jika ingin meretas kode yang sama dengan set karakter set"ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*( )-_+=~`[]{}|\:;"'<>,.?/", jumlah kunci akan dihasilkan akan naik menjadi 6823331935124.

Brute Force attack melakukan perbandingan string matching antara pattern dengan text per karakter dengan pseudocode

DOI: https://doi.org/10.29103/techsi.v10i1.606

berikut : do if (text letter == pattern letter) compare next letter of pattern to next letter of text else move pattern down text by one letter while (entire pattern found or end of text) Exhaustive key search cracking mungkin saja memerlukan waktu yang sangat panjang untuk berhasil, tetapi jika character setnya sidah benar sesaui kode, maka tinggal hanyalah jadi masalah waktu.

Perbandingan panjang kunci dengan jumlah permutasi Key size dalam bits Permutasi 8 28 40 240 56 256 64 264 128 2128 256 2256 2.2 Algoritma Simetrik Symmetric cipher dengan kunci 64 bit atau tidak terlalu rentan terhadap brute force attack. DES, blok cipher digunakan secara luas yang menggunakan 56-bit kunci, dirusak oleh proyek EFF (Electronic Frontier Foundation) pada tahun 1998, dan pesan RC5 kunci 64- bit baru-baru ini sudah berhasil dipecahkan. Banyak orang berpikir bahwa organisasi-organisasi yang didanai dengan baik, terutama lembaga SIGINT(Signals and Intellegence) pemerintah seperti US NSA(National Security Agency), berhasil dapat menyerang sebuah sandi kunci simetris dengan kunci 64-bit dengan menggunakan Brute Force Attack. Untuk aplikasi yang memerlukan keamanan jangka panjang, 128 bit, pada tahun 2004, saat ini sedang dipikirkan panjang kunci yang cukup dan kokoh untuk sistem baru menggunakan algoritma kunci simetrik. NIST(National Institute of Standards) telah merekomendasikan bahwa 80-bit desain akan berakhir pada tahun 2015. Bahkan dalam situasi adalah128-bit atau kunci yang lebih besar digunakan dengan cipher yang dirancang dengan baik seperti AES, Brute Force dapat dilakukan untuk meretas jika kunci tidak dihasilkan dengan benar. Banyak keamanan produk komersial dan shareware yang bangga mengiklankan "keamanan 128-bit" kunci berasal dari sebuah kata sandi yang dipilih pengguna atau passphrase.

Karena pengguna jarang menggunakan kode dengan hampir 128 bit entropi, sistem seperti seringkali cukup mudah untuk dibobol dalam prakteknya. Beberapa produk keamanan bahkan membatasi jumlah masukan karakter maksimum

DOI: https://doi.org/10.29103/techsi.v10i1.606

pengguna sampai ke panjang yang terlalu kecil untuk sebuah passphrase.

Berikut adalah beberapa contoh kode atau passphrase yang dihasilkan dengan metode yang memberikan keamanan 128-bit:

• kode 28-huruf acak dengan semua huruf tunggal kasus: "sqrnf oikas ocmpe vflte krbqa jwf"

• 20 karakter acak kode dengan huruf campuran- kasus, angka dan karakter khusus: ". iTb \ /&/-} itu / P; ^ +22 q"

• 10 acak-dipilih-kata Diceware(hardware number generator) dengan kata sandi: " serf bare gd jab weld hum jf sheet gallop neve" Hampir tidak ada yang menggunakan kode yang sekompleks ini. Salah satu solusinya adalah untuk menerima kekuatan yang lebih rendah. 16 huruf atau 6 kata diceware akan memberikan keamanan yang 75-bit, cukup untuk melindungi terhadap semua semua kecuali kriptoanalisis paling kuat. Solusi lain adalah dengan menggunakan fungsi derivasi kunci (KDF) atau "key stretcher" yang melakukan pekerjaan komputasi yang signifikan dalam mengkonversi kode menjadi kunci, membuat penyerang brute force mengulang ini bekerja untuk setiap percobaan kunci. Dalam prakteknya, teknik ini dapat menambah 10 sampai 20 bit kekuatan untuk kode, cukup untuk memungkinkan sebuah passphrase yang cukup diingat untuk digunakan, tetapi tidak cukup untuk mengamankan kata sandi yang pendek kebanyakan orang pakai. Sayangnya, masih sedikit yang menggunakan produk keamanan teknologi KDF. Mungkin solusi terbaik adalah untuk menyimpan kunci yang dihasilkan secara acak dan kekuatan dalam dan bagian internal dilindungi oleh kode atau PIN.

III. HASIL DAN PEMBAHASAN

Enkripsi

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption)[3].Ciphertext adalah pesan yang sudah tidak dapat

DOI: https://doi.org/10.29103/techsi.v10i1.606

dibaca dengan mudah. Terminologi yang lebih tepat digunakan adalah "encipher".

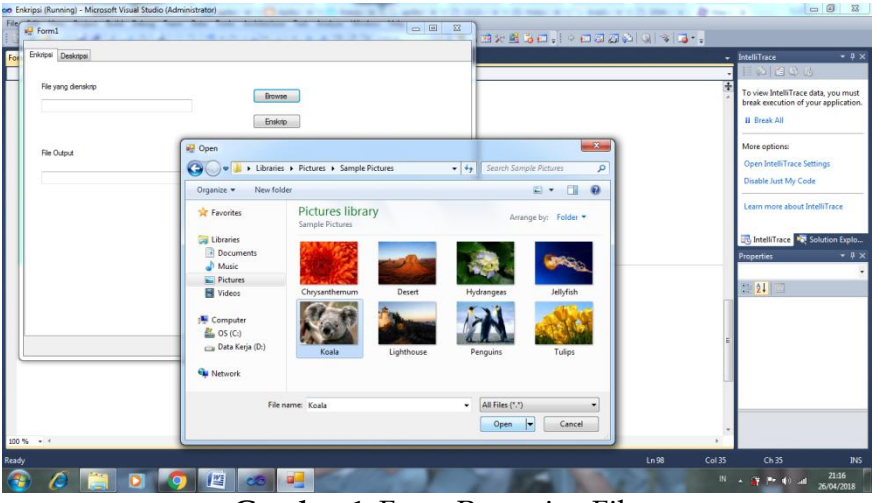
Deskripsi

Proses dekripsi merupakan proses untuk mengembalikan file kembali ke bentuk semula dan untuk mengubah ciphertext menjadi plaintext.

3.1 Hasil

Pembangunan form pada tulisan ini dibuat dengan pemrograman Visual Basic .Net 2010. Pada aplikasi ini proses enkripsi dan dekripsi tidak dipisahkan halamannya, melainkan dipisahkan oleh komponen TabControl. Pada halaman dibawah terdapat beberapa tombol yang berfungsi:

1) Button 1 Tombol ini merupakan tombol Browse pada tab Enkripsi yang berfungsi untuk mencari file yang ingin di enkripsi. Jika tombol tersebut diklik maka akan muncul tampilan seperti dibawah ini.



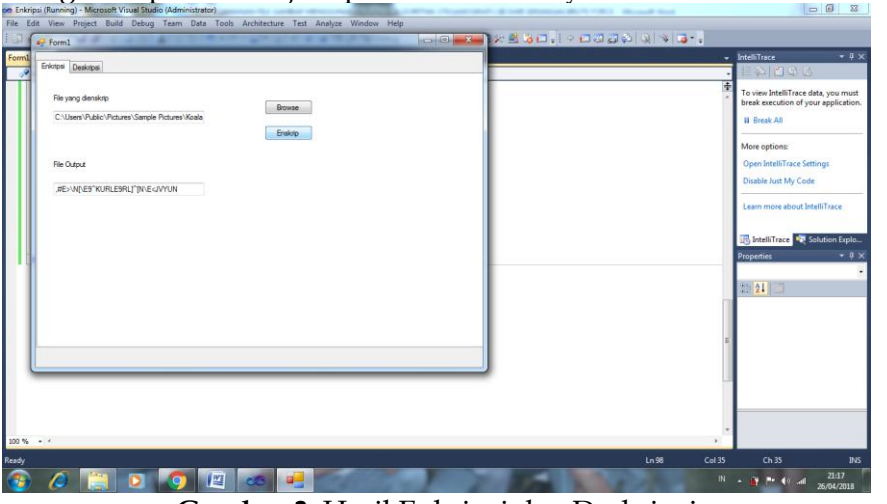
Gambar 1. Form Pencarian File

DOI: https://doi.org/10.29103/techsi.v10i1.606

Gambar 2. Form Input Password

Gambar diatas merupakan form input password, password yang bisa dimasukkan minimal 8 karakter. Setiap file memiliki passwordnya masing-masing, jadi setiap file yang terenkipsi passwordnya berbeda-beda. Pilih OK untuk enkripsi.

2) Button 2 merupakan tombol Enkripsi yang berfungsi untuk mengubah pesan menjadi pesan tersembunyi.



Gambar 3. Hasil Enkripsi dan Deskripsi

DOI: https://doi.org/10.29103/techsi.v10i1.606

Gambar diatas menunjukkan aplikasi berjalan lancar. Begitu pula dengan proses enkripsi dan dekripsinya.

IV. KESIMPULAN

Penggunaan Algoritma Steganografi LSB dapat digunakan untuk memberi keamanan pada data berupa gambar, sehingga dengan menggunakan algoritma steganografi LSB semua file gambar dapat teramankan dari serangan brute force.

DAFTAR PUSTAKA

Gunawan, I. "PENGGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYAPADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS".InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan) Vol 1, No 1, September 2016.

Ariyus. D. Keamanan Multimedia. Yogyakarta : Andi. 2009.

Aulia, N. APLIKASI ENKRIPSI DAN DEKRIPSI MENGGUNAKAN VISUAL BASIC 2012 DENGAN ALGORITMA TRIPLE DES,20 Mei 2016.

DOI: https://doi.org/10.29103/techsi.v10i1.606