ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 05, Number: 01, April 2021 ISSN 2598-6341 (online)

Kriptografi dan Steganografi Penyembunyian Pesan Pada Media Audio Menggunakan Algoritma AES

[1] Lambok Hasudungan Sijabat, [2] Nenna Irsa Syahputri, [3] Mufida Khairani
Program Studi Teknik Informatika Fakultas Teknik dan Komputer Universitas Harapan Medan
Jl. HM Jhoni No. 70 Medan, Indonesia[1,2,3]
Email:[1]lsijabat1998@gmail.com,[2]nenna.ziadzha@gmail.com,[3]mufida.khairani@gmail.com

Abstract

Cryptography can be used to process messages with certain algorithms so that the meaning of the message is difficult to understand. After that, *steganography* was used to hide messages in other forms. This study uses *AES* and *Least Significant Bit (LSB)* to build desktop-based applications using VB to send messages and get original messages. This application itself will concentrate the application of dual security for data and use WMA audio files to strengthen security on text data owned by users. Conceptually, security will be carried out by first encrypting messages using *AES cryptography* and then continuing the second security process by inserting text data in the WMA Audio file using the *LSB algorithm* to prevent indication or suspicion of the existence of important data or information that is inserted in the data.

Keywords : *Cryptography, Steganography, AES, LSB*

Abstrak

Kriptografi dapat digunakan memproses pesan dengan algoritma tertentu sehingga makna dari pesan tersebut sulit dimengerti. Setelah itu, *steganografi* digunakan untuk menyembunyikan pesan dalam bentuk lain. Penelitian ini menggunakan *Algoritma AES* dan *Least Significant Bit (LSB)* untuk membangun aplikasi berbasis desktop menggunakan VB untuk mengirim pesan dan mendapatkan pesan asli. Aplikasi ini sendiri akan memusatkan penerapan pengamanan ganda bagi data dan menggunakan file audio WMA untuk memperkuat pengamanan pada data teks yang dimiliki oleh pengguna. Secara konsep, pengamanan akan dilakukan dengan mengenkripsi pesan terlebih dahulu dengan menggunakan *kriptografi AES* dan kemudian melanjutkan proses pengamanan kedua dengan menyisipkan data teks pada file Audio WMA menggunakan algoritma *LSB* untuk mencegah indikasi atau kecurigaan terhadap adanya data atau informasi penting yang disisipkan pada data.

Kata Kunci: *Kriptografi, Steganografi, AES, LSB*

1. PENDAHULUAN

Kriptografi merupakan seni dan ilmu untuk menulis rahasia *"The Art of Secreet Writing".* Tujuan dari *kriptografi* adalah mengolah informasi dengan algoritma tertentu supaya pesan tidak dapat dibaca. Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) disebut dengan enkripsi (*encryption*). *ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah atau sulit dimengerti maknanya. Proses untuk mengembalikan atau mengubah *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*).

Namun penggunaan *kriptografi* sering menimbulkan kecurigaan pihak ketiga, sebab pesan yang sulit dimengerti pasti sudah diolah dan menunjukkan bahwa pesan itu merupakan informasi penting. Apalagi saat ini semakin berkembang kemampuan untuk memecahkan *kriptografi* yang disebut krpitanalisis. [1].

Untuk menghindari permasalahan tersebut maka terciptalah *steganograf*i yaitu metode menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video. Aspek terpenting dari *steganografi* adalah tingkat keamanan penyembunyian informasinya, yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi.[2].

Steganografi yang umum digunakan adalah penyembunyian informasi pada media gambar, di mana informasi text dimasukkan ke dalam bit pixel gambar. Namun metode yang sering digunakan masih cukup sederhana sehingga pihak ketiga masih bisa mendapatkan informasi yang disembunyikan.[3].

Untuk menghindari permasalahan tersebut maka terciptalah *steganograf*i yaitu metode menyembunyikan informasi pada sebuah media, bisa berupa media gambar, suara ataupun video. Aspek terpenting dari *steganografi* adalah tingkat keamanan penyembunyian informasinya, yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi.

Steganografi yang umum digunakan adalah penyembunyian informasi pada media gambar, di mana informasi text dimasukkan ke dalam bit pixel gambar. Namun metode yang sering digunakan masih cukup sederhana sehingga pihak ketiga masih bisa mendapatkan informasi yang disembunyikan.

2. LANDASAN TEORI

A.Kriptografi

Kriptografi Kriptografi terdiri dari dua kata yang berasal dari bahasa Yunani, yaitu: *"kryptos"* dan *"graphia"*. Arti kata *"kryptos"* adalah sesuatu yang disembunyikan, tidak dikenal, terselubung, rahasia atau misterius. Sedangkan *"graphia"* berarti tulisan. Jadi, *kriptografi* dapat dijelaskan secara harfiah sebagai tulisan rahasia atau terkadang disebut sebagai seni dan ilmu tulisan rahasia. Menurut buku yang berjudul "Applied Cryptography" karangan Bruce Schneider [4]. *kriptografi* merupakan suatu seni atau ilmu untuk menjaga kerahasiaan dari sebuah tulisan agar tetap aman, tanpa diketahui pihak yang tidak berkepentingan. Pakar ilmu *kriptografi* dikenal sebagai kriptografer. Selain *kriptografi*, ada kripanalisis yang merupakan kebalikan dari proses *kriptografi* dalam kriptologi.

B.Steganografi

Steganografi adalah sebuah seni menyembunyikan pesan rahasia dengan tujuan agar keberadaan pesan rahasia tersebut tidak diketahui oleh orang yang tidak berkepentingan. Ada dua proses utama dalam *steganografi* yaitu proses penyisipan dan proses pengekstrakan. *Steganografi* menggunakan sebuah berkas yang disebut dengan *cover* atau biasa disebut dengan *carrier*, tujuannya sebagai media pembawa dari pesan rahasia.

C.Algoritma AES

Algoritma AES Rijndael ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaimana *block cipher* pada umumnya. Menurut jenisnya AES terbagi tiga jenis, yaitu:

1. AES-128
2. AES-192
3. AES-256

Pengelompokkan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tiap-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya *round* yang dipakai. AES-128 menggunakan 10 *round*, AES-192 sebanyak 12 *round*, dan AES-256 sebanyak 14 *round*.

D.Visual Basic 2010

Visual Basic 2010 adalah sebuah bahasa pemrograman berbasis OOP atau *object oriented programming* yang memanfaatkan teknologi .NET yang digunakan untuk membuat aplikasi di lingkungan kerja berbasis Windows. Visual Basic 2010 atau Visual Basic .NET 2010 merupakan pengembangan dari versi visual basic sebelumnya, dibandingkan dengan versi sebelumnya Visual Basic 2010 telah menggunakan antar muka pengguna yang canggih dan teknologi .NET terbaru yaitu .NET 4.0.

3 . METODE PENELITIAN

AES memiliki ukuran blok yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran blok yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap *plainteks* akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal, kemudian blok itu akan diproses dengan metode berikutnya. Metode yang digunakan dalam algoritma ini yaitu *add round key, subbytes, shift rows, mix columns.*

Transformasi *SubBytes* : merupakan operasi substitusi non-linier pada tiap-tiap *byte* dalam *state* dengan menggunakan tabel substitusi yang dinamakan *S-box* (kotak S), bisa dilihat tabel di bawah berikut.

St4

66	75	7A	7C
79	7B	79	76
79	64	7D	71
75	74	71	7E

Tabel 1 Proses *SubBytes*

Transformasi *ShiftRows* : pergeseran baris-baris pada kolom kotak 4 X 4 menggeser dengan cara memutar *byte-byte* pada baris 1, 2, dan 3 dari *state* dengan jumlah pergeseran yang bervariasi bisa diliha tabel di bawah berikut.

33	9D	DA	10
B6	21	B6	38
B6	43	FF	FF
9D	92	A3	F3

St5

Geser 1 byte

Geser 2 byte

Geser 3 byte

33	9D	DA	10
21	B6	38	B6
FF	FF	B6	43
F3	9D	92	A3

Tabel 2 *ShiftRows*

Transformasi *MixColumn* : adalah perkalian terhadap matriks konstan yang dioperasikan pada kolom-kolom kotak 4 X 4 bisa dilihat tabel di bawah berikut.

09	82	C3	01
98	6D	F9	01
F9	72	38	DE
76	D4	C4	98

Tabel 3 *Mixcolumns*

Transformasi *AddRoundKey* : dengan cara menambahkan kunci ronde ke *state* dalam operasi XOR.
Pada perputaran terakhir, transformasi *MixColumn* tidak digunakan, karna sudah aturan ketetapannya, bisa dilihat tabel di bawah berikut.

AddRoundKey

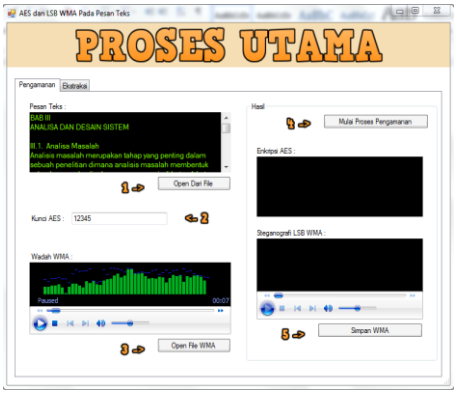
66	75	79	7E
79	7B	79	7E
76	65	7E	78

32	30	32	30
30	30	30	30
30	30	30	30
30	30	30	30

Tabel 4 *AddRoundKey*

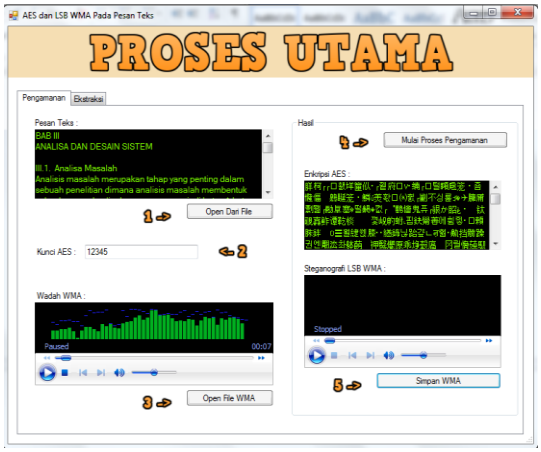
4. HASIL DAN PEMBAHASAN

Pada halaman ini pengguna harus terlebih dahulu melakukan input data plain data pada sistem dan kemudian menginputkan password yang akan digunakan untuk mengenkripsi data teks. Selanjutnya pengguna akan menginputkan data audio dengan ekstensi WMA (sesuai dengan kebutuhan sistem) yang akan digunakan sebagai media steganografi. Penulis telah menyiapkan tes yaitu data WMA dengan nama yang akan digunakan pada proses enkripsi dengan nama Dan Farber - Don-t Touch.WMA langkah selanjutnya adalah menginputkan teks dan file audio uji kedalam sistem.



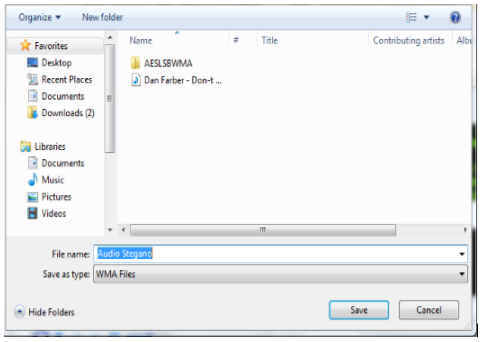
Gambar 1 Input Data Kedalam Sistem

Setelah data uji teks dan data uji audio selesai diinputkan langkah selanjutnya adalah melakukan proses pengamanan. Pada proses pengamanan ini, password yang digunakan adalah "12345". Berikut tampilan dari hasil proses pengamanan:



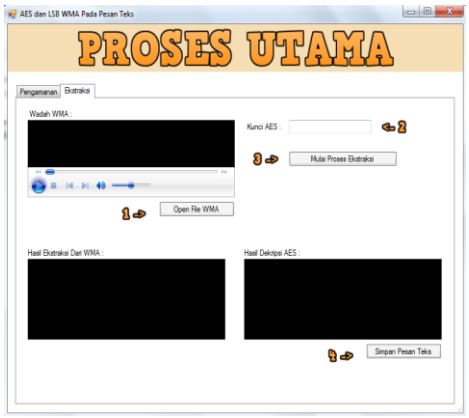
Gambar 2 Hasil Pengamanan Data

Pada gambar diatas dapat dilihat bahwa proses pengamanan sudah berhasil dilakukan. Pada halaman hasil pengamanan akan ditampilkan dalam dua bagian yaitu enkripsi AES dan Steganografi LSB WMA. Pada bagian enkripsi AES, akan ditampilkan hasil enkripsi data teks dengan menggunakan algoritma AES, sedangkan pada bagian steganografi akan diputar file audio hasil steganografi LSB untuk menunjukkan bahwa tidak adanya perubahan yang tampak pada data. Setelah proses pengamanan selesai, langkah selanjutnya adalah dengan menyimpan data hasil stegano.



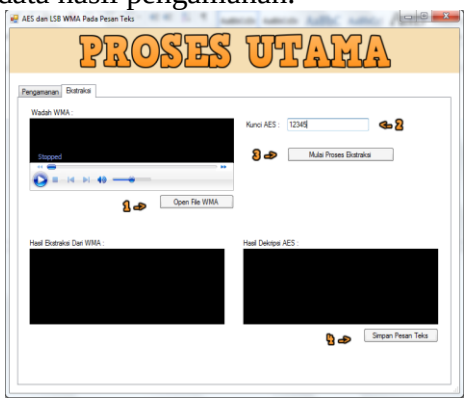
Gambar 3 Penyimpanan Data hasil Pengamanan

Setelah data hasil pengamanan selesai disimpan, langkah selanjutnya adalah melakukan proses ekstraksi terhadap data yang diamankan berikut tampilan halaman dekripsi.



Gambar 4 Halaman Ekstraksi

Menampilkan antarmuka yang digunakan untuk mengekstraksi kembali data-data hasil pengamanan untuk mengembalikan informasi yang sebelumnya sudah diacak dan tidak dapat dibaca menjadi kondisi semula dimana data-data dan informasi kembali pada state awal sehingga informasi yang ada didalam file tersebut dapat diakses kembali. Untuk memulai proses ekstraksi pertama pengguna akan memuat data hasil pengamanan yaitu audio stegano kedalam sistem, berikut tampilan load data hasil pengamanan.



Gambar 5 Input Audio Stegano

Setelah data audio stegano selesai di upload kedalam sistem selanjutnya pengguna menginputkan password yang digunakan sebelumnya dan kemudian akan menekan tombol mulai proses ekstraksi untuk mengekstraksi data teks dari dalam audio dan kemudian mendekripsi chiperteks tersebut kembali pada kondisi semula. Berikut tampilan dari program saat dekripsi sudah berhasil dilakukan.

Gambar 6 Hasil Ekstraksi Data

Setelah proses Ekstraksi selesai dilakukan maka akan muncul pesan bahwa dekripsi sudah berhasil. Perlu diingat bahwa setiap d Ekstraksi yang dilaksanakan pada sistem ini akan dilabelkan sebagai proses Ekstraksi yang berhasil. Hal ini dikarenakan sistem yang tidak menampilkan data asli pada saat Ekstraksi dikarenakan untuk menjaga sistem agar bersih dari history atau pentunjuk akan kondisi data sebelumnya. Setelah selesai di dekripsi langkah selanjutnya adalah menyimpan data hasil dekripsi kedalam komputer.

5. KESIMPULAN

Dalam perancangan, pembuatan, dan pengujian aplikasi Kriptografi dan Steganografi pada penyembunyian pesan pada media audio WMA menggunakan Algoritma AES terdapat beberapa kesimpulan yang dapat diambil oleh penulis, diantaranya adalah sebagai berikut :

1. Perancangan dan juga implementasi pembuatan program telah berhasil dilaksanakan dan menghasilkan program yang diinginkan dengan menerapkannya dengan bahasa pemograman Visual Studio 2010.
2. Penggunaan file audio WMA pada aplikasi berhasil menyembunyikan data atau informasi rahasia kedalamnya tanpa memberikan perubahan yang berarti atau signifikan pada data audio sehingga tidak menimbulkan kecurigaan terhadap data rahasia didalamnya.
3. Penggunaan data Text (.txt) yang digunakan memastikan sistem hanya melakukan proses steganografi terhadap data yang bersifat teks. Penggunaan ekstensi ini memastikan penggunaan LSB yang ada pada audio wma dapat dilakukan dengan optimal dan tidak melebihi kapasitas kemampuan penampungan data audio.
4. Secara ukuran, data audio hasil steganografi tidak memiliki perubahan ukuran yang berarti. Perubahan ukuran data dari hasil proses steganografi akan sangat tergantung terhadap jumlah atau panjang pesan yang disisipkan kedalam data stegano, dimana makin besar data stegano yang disisipkan kedalam data maka makin besar perubahan ukuran data.

DAFTAR PUSTAKA

[1] Ariyus, D. Keamanan “Multimedia. Yogyakarta,”: Penerbit Andi. no. 1, pp. 65–66, 2017.

[2] Chasanah, Zulfah. Steganografi Pada File Audio MP3 Untuk Pengamanan Data Menggunakan Metode Least Significant Bit (LSB). Skripsi. Malang, Indonesia: “Universitas Islam Negeri,”. no. , pp. 2301–9425, 2018.

[3] Jes´Us D´Iaz Vico. Steganography And Steganlaysis: Data Hiding In Vorbis Audio Streams. Facultad De Inform´Atica Universidad Polit´Ecnica De Madrid. no. 59 , pp. 297–303, 2010.

[4] Schneier, Bruce; “Applied Cryptography Second Edition: protocol, algorithm, and source code in C”; John Wiley and Son , 1996.