ISSN 2355-3286

Implementasi Audio Steganografi menggunakan 4th LSB dan Advanced Encryption Standard pada Windows Phone

M. Chaeril Maricar, Seng Hansun
Program Studi Teknik Informatika, Universitas Multimedia Nusantara, Tangerang, Indonesia
chaeril@live.com, hansun@umn.ac.id

Diterima 17 Februari 2015
Disetujui 30 April 2015

Abstract—Securing data during transmission become one of the problem in technology, those data can be intercepted and read by others. One preventive action to overcome this is by using steganography. This thesis implements an audio steganography using Windows Phone. Combination of Advanced Encryption Standard to secure data and Audio Wave Steganography which embedded data inside 4th LSB layer, resulting in increased safety and robustness against noise addition compared to 1st LSB.

Index Terms—Advanced Encryption Standard, Audio Steganography, Audio Wave Steganography, Least Significant Bit, Windows Phone.

I. PENDAHULUAN

Pada zaman sekarang, teknologi merupakan salah satu bidang yang terus berkembang dalam rangka pemenuhan kebutuhan manusia. Komputer, perangkat mobile, jaringan, dan teknologi informasi keamanan adalah bagian dari teknologi yang berkembang pesat. Orang-orang mulai menciptakan dan berbagi data-data multimedia karena adanya kemudahan dan fleksibilitas perangkat lunak [1]. Selain itu, faktor harga data-data digital yang terus menurun juga mempengaruhi hal tersebut. Penggunaan alat rekam dan perangkat penyimpanan juga mempercepat perkembangan multimedia [2].

Dengan pesatnya perkembangan multimedia, kepentingan untuk memproteksi data digital dari pengguna yang tidak sah mulai dibutuhkan, salah satunya ialah dengan menyembunyikan data di dalam data digital lainnya atau biasa disebut sebagai steganografi. Selain itu, dapat juga dilakukan pengacakan bit data digital dengan menggunakan Key. Tindakan ini disebut sebagai enkripsi. Kekurangan enkripsi adalah orang dapat mengetahui bahwa data tersebut sedang dikirim (tidak dapat dicegah), sehingga data yang telah di-enkripsi masih dapat ditangkap dan dianalisis. Namun demikian, tanpa key, enkripsi tidak dapat dipecahkan [3].

Dibandingkan dengan enkripsi, steganografi merupakan metode pengamanan data yang memiliki pendekatan berupa pengiriman informasi yang disembunyikan dalam media lain [4]. Steganografi tidak hanya merujuk pada media digital, tetapi juga media lainnya. Menurut Kessler [5], ada banyak sekali metode steganografi mulai dari sesuatu seperti tinta tak terlihat, mikrodots, hingga menyembunyikan pesan pada setiap huruf kedua pada pesan teks yang besar dan spread spectrum. Sederhananya, apabila pesan yang terenkripsi dikirim, pesan tersebut dapat menarik perhatian dari pihak yang tidak diinginkan. Dengan menggunakan steganografi, pengiriman pesan tersebut tidak akan menimbulkan kecurigaan [3].

Penelitian ini menggunakan metode steganografi, yang ditemukan oleh Ajay B. Gadicha, dengan nama audio wave steganography. Metode ini mencoba mengeksplorasi bit rate ke-4 pada Least Signification Bit audio steganography yang mampu mengurangi distorsi dari penyembunyian data pada host audio. Dengan algoritma ini data disembunyikan dalam lapisan ke-4 Least Signification Bit dan menghasilkan peningkatan ketahanan akan distorsi [6]. Tidak seperti metode Least Signification Bit (LSB) yang tidak efektif karena rentannya terhadap serangan untuk mendapatkan pesan yang disembunyikan, Least Signification Bit juga memiliki kerentanan terhadap distorsi oleh high average power [4].

Metode ini menggunakan pendekatan dua langkah. Pada pendekatan pertama, bit yang di steganografi ditanam kedalam 4th Least Signification Bit host audio, kemudian pada langkah kedua noise yang ditimbulkan oleh penanaman dibentuk agar dapat mengubah sifat dari white noise [6].

Selanjutnya makalah penelitian ini disusun dalam urutan penulisan sebagai berikut, Bab II menjelaskan

tinjauan pustaka utama yang digunakan dalam penelitian ini, meliputi Windows Phone, Free Lossless Audio Codec (FLAC), Kriptografi, Advanced Encryption Standard (AES), Steganografi, dan Least Significant Bit (LSB). Bab III menjelaskan perancangan sistem yang dipersiapkan dalam penelitian ini, yang selanjutnya diterapkan sebagaimana yang dijelaskan dalam Bab IV mengenai implementasi sistem. Hasil penelitian yang dilakukan disari dan dijelaskan dalam Bab V, mengenai simpulan penelitian yang telah dilakukan.

II. TINJAUAN PUSTAKA

A. Windows Phone

Windows Phone merupakan penerus dari Windows yang dikembangkan oleh Microsoft, Windows Mobile menggunakan kernel yang berdasarkan pada Windows CE dan Windows NT (untuk versi Windows Phone 8 keatas).

B. Free Lossless Audio Codec (FLAC)

FLAC merupakan codec untuk melakukan kompresi pada audio lossless. Yang dapat mengurangi ukuran file audio hingga 50- 60% dari ukuran aslinya dan hasil dekompresi yang identik dengan audio data aslinya. Karena keterbatasan API, aplikasi ini menggunakan library FlacBox dalam melakukan pembacaan file FLAC.

C. Kriptografi

Menurut Rahayu [7], Kriptografi merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak. Kata cryptography berasal dari kata Yunani kriptos (tersembunyi) dan graphein (menulis).

D. Advanced Encryption Standard

Advanced Encryption Standard merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok ciphertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi mengubah data menjadi tidak dapat lagi dibaca tersebut ciphertext; sebaliknya dekripsi adalah mengubah ciphertext data menjadi bentuk semula yang dikenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, atau 256 bits untuk mengenkripsi dan mendekripsi data [8].

E. Steganografi

Menurut Kawaguchi [9], Steganografi adalah teknik menyembunyikan bukti nyata hasil perubahan data.

Kessler [5] mengungkapkan steganografi sebagai ilmu menyembunyikan informasi. Jika tujuan dari kriptografi adalah membuat data tidak dapat dibaca oleh pihak yang tidak berhak, maka tujuan dari steganografi adalah menyembunyikan data dari pihak yang tidak berhak.

Menurut Almohammad [10] steganografi memiliki 2 aspek utama yaitu steganographic capacity dan imperceptibility. Kedua aspek ini berbanding terbalik, cukup sulit untuk meningkatkan steganographic capacity dan secara bersamaan menjaga imperceptibility. Imperceptibility merupakan kriteria saat data asli dan data hasil tidak dapat dibedakan secara perseptual.

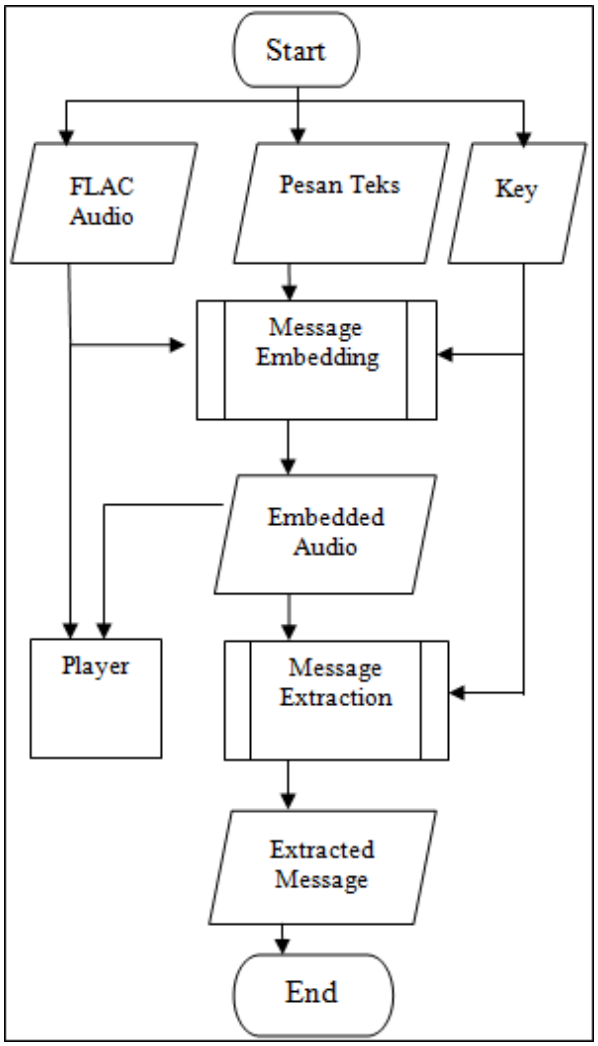
F. Least Significant Bit (LSB)

Least significant bit adalah bit dalam binary integer yang menentukan apakah angka tersebut merupakan bilangan ganjil atau genap, Least significant bit sendiri biasa disebut sebagai bit paling kanan pada binary. Bit tersebut merupakan bit yang memiliki nilai potensial paling sedikit [11].

III. PERANCANGAN SISTEM

A. Diagram Sistem

Prosedur kerja sistem secara umum dapat dijelaskan dengan lebih mudah menggunakan diagram. Pada intinya ada dua prosesyang saling berurutan yaitu teks embedding dan teks extraction. Setiap proses tersebut adalah proses yang sudah terdefinisi (predefined process) dan harus dikerjakan (mandatory). Data yang dikirimkan dari proses teks embedding ke proses teks extraction merupakan audio yang sudah di-steganografi.



Gambar 1. Flowchart umum sistem

IV. IMPLEMENTASI SISTEM

A. Implementasi Sistem

Sistem diimplementasikan berdasarkan rancangan yang telah dibuat sebelumnya. Implementasi dimulai dengan memprogram class-class yang mendeklarasikan metode-metode Advanced Encryption Standard, dan Steganografi. Pembuatan class-class ini bertujuan untuk meningkatkan reusability dari kode dan keteraturan pemrograman. Implementasi dilanjutkan dengan memprogram antarmuka untuk aplikasi Windows Phone.

Tahap terakhir adalah memprogram fungsionalitas dari aplikasi yaitu modul-modul utamanya dengan memanfaatkan class-class yang telah ada dan diintegrasikan dengan antarmuka yang dibuat sebelumnya. Seperti yang telah dijelaskan sebelumnya, class-class yang dibuat hanya berisi fungsi-fungsi untuk mengimplementasikan algoritma yang digunakan. Beberapa proses dalam rancangan yang tidak berkaitan dengan algoritma tersebut diimplementasikan menggunakan function dan blok program yang sifatnya khusus untuk modul tertentu. Implementasi modul selalu dilanjutkan dengan unit test untuk memastikan kinerja aplikasi. Aplikasi yang dikembangkan diberi nama "Audio Steganography".

B. Hasil Implementasi

Berikut ini merupakan hasil implementasi sistem yang dirancang pada aplikasi Audio Steganography berbasis Windows Phone. Beberapa pivot item yang ada dalam aplikasi Audio Steganography adalah sebagai berikut.

• Encode: halaman Encode berisi sebuah list picker untuk memilih audio yang akan digunakan, dua buah textbox masing masing digunakan untuk mengisi pesan yang akan dikirim dan password untuk mengenkripsi pesan tersebut, dan sebuah button untuk memulai atau membatalkan proses.

• Decode: halaman Decode berisi sebuah list picker untuk memilih audio yang akan digunakan, dua buah textbox masing masing digunakan untuk mengisi password untuk melakukan dekripsi pesan dan menampilkan pesan yang tersembunyi, dan sebuah button untuk memulai atau membatalkan proses.

• Player: halaman Player berisi sebuah list picker untuk memilih audio yang akan dimainkan, dua buah button masing masing digunakan untuk memainkan lagu dan menghentikan lagu. Halaman ini digunakan untuk melakukan pengujian pada audio sebelum dan sesudah di-steganografi

• Share: halaman Share berisi dua buah list picker masing masing digunakan untuk memilih audio yang akan dikirim dan memilih recipient untuk melakukan pengiriman melalui Bluetooth, dan 3 buah tombol yang digunakan untuk mengirim file melalui Bluetooth, melakukan Sign-in dan upload ke OneDrive.

• Resource: halaman Resource berisi lima buah textblock masing masing digunakan untuk menampilkan device memory, ukuran audio yang dapat diproses, batasan memory pada aplikasi, memory peak dan memory usage aplikasi.

V. SIMPULAN

Berdasarkan hasil implementasi dan uji coba yang telah dilakukan, simpulan penelitian ini adalah sebagai berikut.

• Aplikasi "Audio Steganography" yang mengimplementasikan audio wave steganography dan Advanced Encryption Standard telah berhasil dibuat.

• Berdasarkan pernyataan para responden audio yang telah di-steganografi tidak mengandung noise.

Tabel 1. Data kemiripan audio oleh responden

Nama Audio	Kemiripan oleh responden					Persentase kemiripan
	I	II	III	IV	V	
01 The Lion Sleeps Tonight	100%	100%	100%	100%	100%	100%
17 Haste to the Wedding	100%	100%	100%	100%	100%	100%
08 – Louise	100%	100%	100%	100%	100%	100%
01 Sims Main Theme (From Sims 3)	100%	100%	100%	100%	100%	100%

DAFTAR PUSTAKA

[1] Citrix. (2012). Retrieved from Citrix Systems, Inc: http://www.citrix.com/site/resources/dynamic/additional/byod_best_practices.pdf

[2] Ethan P. White, E. B. (2014). Nine simple ways to make it easier to (re)use your data. Retrieved from Nine simple ways to make it easier to (re)use your data: http://blog.martinfenner.org/2013/06/25/nine-simple-ways-to-make-it-easier-to-reuse-your-data/

[3] Oriyano, S.-P. (2009). Using steganography to avoid observation. Retrieved from IBM Developerworks: ibm.com/developerWorks/.

[4] Nosrati, M., Karimi, R., & Hariri, M. (2012). Audio Steganography: A Survey on Recent Approaches. World Applied Programming, 202-205.

[5] Kessler, G.C. (2013). Steganography: Hiding Data Within Data. Retrieved from Gary Kessler: http://www.garykessler.net/library/steganography.html.

[6] Ajay.B.Gadicha. (2011). Audio Wave Steganography. International Journal of Soft Computing and Engineering (IJSCE), 174-176.

[7] Rahayu, F. S. (2013). Cryptography. Retrieved from http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/124/124P-04-final2.0-Cryptography.pdf.

[8] FIPS. (2001). Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards Publication 197.

[9] Kawaguchi, E. & Richard E.O. (2013). Principle and Applications of BCPS-Steganography. Retrieved from Datahie: http://web.eece.maine.edu/~eason/steg/SPIE98.pdf.

[10] Almohammad, A. (2010). Steganography-Based Secret and. Retrieved from brunel: http://v-scheiner.brunel.ac.uk/bitstream/2438/4634/1/FulltextThesis.pdf.

[11] Microsoft Corp. (2014). IBM SNA Formats Bit Ordering is Opposite of Intel Convention. Retrieved from Microsoft Support: http://support.microsoft.com/kb/130861.