APLIKASI KRIPTOGRAFI AUDIO MENGGUNAKAN PEMBANGKIT KUNCI BERBASIS SIDIK JARI DAN *ADVANCED ENCRYPTION STANDARD*

SKRIPSI

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
pada Jurusan Ilmu Komputer / Informatika

Disusun oleh:

T. Han Setiawan O

J2F009072

JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2015

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama : T. Han Setiawan O

NIM : J2F009072

Judul : Aplikasi Kriptografi Audio menggunakan Pembangkit Kunci berbasis Sidik Jari dan *Advanced Encryption Standard*

Dengan ini saya menyatakan bahwa dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 20 Agustus 2015

T. Han Setiawan O

J2F009072

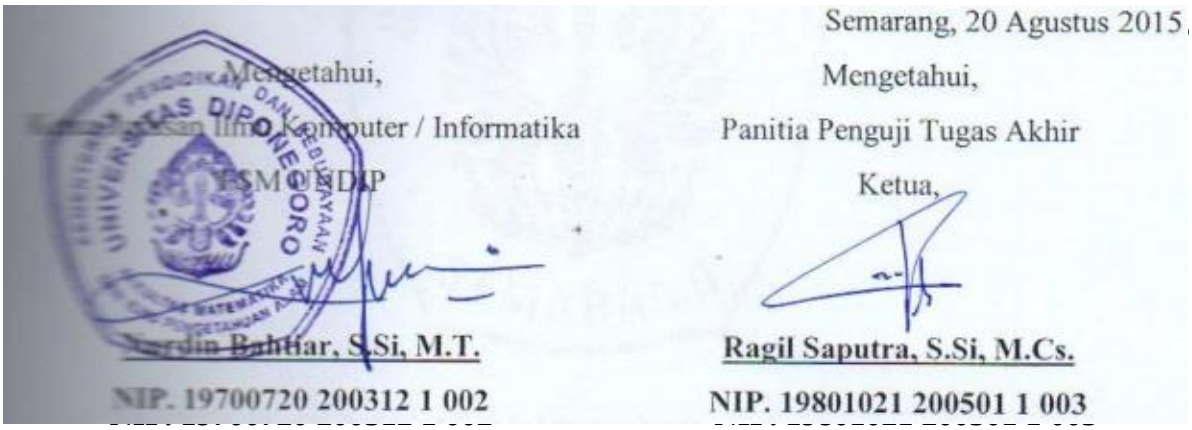
HALAMAN PENGESAHAN

Judul : Aplikasi Kriptografi Audio menggunakan Pembangkit Kunci berbasis Sidik Jari dan *Advanced Encryption Standard*

Nama : T. Han Setiawan O

NIM : J2F009072

Telah diujikan pada sidang tugas akhir pada tanggal 10 Agustus 2015 dan dinyatakan lulus pada tanggal 20 Agustus 2015.



HALAMAN PENGESAHAN

Judul : Aplikasi Kriptografi Audio menggunakan Pembangkit Kunci berbasis Sidik Jari dan *Advanced Encryption Standard*

Nama : T. Han Setiawan O

NIM : J2F009072

Telah diujikan pada sidang tugas akhir pada tanggal 10 Agustus 2015.

Semarang, 20 Agustus 2015

Dosen Pembimbing,

Aris Sugiharto, S.Si, M.Kom

NIP. 19710811 199702 1 004

ABSTRAK

Penggunaan kata kunci yang berkaitan dengan informasi sosial seseorang seperti tanggal lahir, nama hewan peliharaan, dan lainnya menyebabkan mudahnya pencurian pada data yang bersifat personal. Tak jarang percakapan melalui saluran yang telah diamankan dengan proses kriptografi pun dapat disadap. Umumnya, kata kunci maupun kunci yang berkaitan dengan proses kriptografi tersebut dapat diketahui dengan melakukan analisa sederhana dan sedikit menebak-nebak apa yang menjadi materi dalam pengaplikasian kunci tersebut. Kombinasi terhadap karakter yang digunakan dalam memasukkan kunci tersebut juga tergolong mudah ditebak. Umumnya digunakan karakter yang mirip dengan huruf tertentu agar pengguna mudah mengingat kunci yang dimiliki. Sidik jari telah lama dikenal sebagai alat bantu identifikasi personal yang bersifat unik dan universal. Semua orang memiliki sidik jari dan tidak ada dua sidik jari yang identik satu sama lain bahkan dari jari-jari pada tangan yang sama. Proses identifikasi sidik jari umumnya dilakukan dengan melakukan ekstraksi terhadap titik minutiae. Titik minutiae merupakan detil terkecil pada sebuah citra sidik jari. Lokasi koordinat dan sudut orientasi tiap titik minutiae pada tiap jari individu memiliki kombinasi yang sangat beragam. Hal inilah yang dapat dijadikan sebagai titik awal pembangkitan kunci kriptografi untuk melakukan proses pengamanan data. *Advanced Encryption Standard* (AES) merupakan standar keamanan yang umum digunakan dalam proses pengamanan data digital. Pengembangan aplikasi kriptografi ini diharapkan mampu menghasilkan kombinasi kunci yang lebih baik dan sesuai dengan ukuran kunci yang dapat ditangani oleh AES. Sehingga, data dapat diamankan secara lebih baik.

Kata Kunci : Sidik jari, titik minutiae, algoritma pembangkit kunci kriptografi, AES.

ABSTRACT

Social information-related passwords such as birthdate, pet name, and any other informations could cause personal data robbery. It is known that even a secured line could be tapped because of this. It took a little analysis and some lucky guess to steal these cryptographical key. The character combination used in the key input is easy to be guessed as well. Usually, characters which associated with 'normal' letters is used to help users memorize their passwords. Fingerprint has been known for years as the universal and unique personal identification tool. There is not even ever existed that two different fingers in a hand have identical patterns. Fingerprint recognition is usually done by extracting minutiae points. Minutiae points is the least details on a fingerprint image. The coordinates and orientations of minutiae points on every individuals' finger is unique to each other. This could mean a possibility of using minutiae points as a starting point to generate cryptographical key. The Advanced Encryption Standard is the common form of digital data security standard. The development of this cryptographical application is expected to generate a more secure key combination which conforms with the key standards of AES. So that the data could be secured better than before.

Keywords : Fingerprint, minutiae points, cryptographical key generator algorithm, AES.

KATA PENGANTAR

Segala puji penulis persembahkan pada Allah SWT atas segala rahmat yang telah dikaruniakan dalam penyusunan tugas akhir. Tugas akhir berjudul '**Aplikasi Kriptografi menggunakan Pembangkit Kunci berbasis Sidik Jari dan *Advanced Encryption Standard***' telah berhasil diselesaikan sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada jurusan Ilmu Komputer/Informatika Universitas Diponegoro.

Laporan tugas akhir ini menjadi dokumentasi terhadap hasil penelitian yang dilakukan pada penyusunan tugas akhir. Tak lupa penulis sampaikan rasa hormat dan terima kasih kepada seluruh pihak yang telah ikut berperan baik secara langsung maupun tidak langsung dalam keberhasilan penyusunan serta penyelesaian tugas akhir dan dokumen laporan ini. Adapun pihak yang terlibat antara lain:

1. Prof. Dr. Widowati, S.Si, M.Si, selaku Dekan Fakultas Sains dan Matematika (FSM) Universitas Diponegoro.
2. Nurdin Bahtiar, S.Si, M.T, selaku Ketua Jurusan Ilmu Komputer/Informatika FSM Universitas Diponegoro.
3. Indra Waspada, S.T., M.T, selaku Dosen Koordinator Tugas Akhir Jurusan Ilmu Komputer/Informatika FSM Universitas Diponegoro.
4. Aris Sugiharto, S.Si, M.Kom, selaku Dosen Pembimbing yang telah banyak memberikan pengarahan dan bimbingan selama proses penyelesaian tugas akhir ini.
5. Serta seluruh pihak yang secara langsung maupun tidak langsung telah ikut berperan dalam penyelesaian tugas akhir ini. Semoga Allah SWT membalas semua kebaikan dengan limpahan rahmat-Nya.

Laporan ini juga disusun sebagai dokumen yang dapat diacu sebagai pertimbangan dalam pengembangan lebih lanjut terhadap topik maupun bidang ilmu terkait topik tugas akhir yang diselesaikan penulis. Penulis juga menyadari banyak ketidaksempurnaan baik dalam hal materi maupun penyajian karena keterbatasan pengetahuan dan kemampuan penulis. Kritik dan saran yang baik sangat diharapkan oleh penulis. Semoga laporan tugas akhir ini dapat memberikan manfaat yang baik bagi pembaca secara umum maupun penulis secara khusus.

Semarang, 20 Agustus 2015

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini memaparkan mengenai latar belakang, rumusan masalah mengenai topik yang diambil, tujuan dan manfaat, ruang lingkup permasalahan dalam tugas akhir dan sistematika penulisan laporan tugas akhir ini.

1.1. Latar Belakang

Sidik jari telah lama digunakan sebagai alat bantu identifikasi yang bersifat unik dan universal. Awalnya, proses pengenalan sidik jari dilakukan untuk keperluan forensik. Mulai dari pengenalan identitas pelaku kejahatan hingga membantu identifikasi sosok jasad manusia yang tak dikenal yang menjadi korban tindak kejahatan. Umumnya, sidik jari didapat dengan meletakkan jari subjek pada tinta, kemudian menempelkan jari tersebut pada kertas kosong agar pola sidik jari tersebut dapat terlihat dengan jelas. Pola yang terdapat pada sidik jari kemudian dikenali dengan mencocokan atau mencatat jenis pola yang terdapat pada citra tersebut. Pola pada sidik jari umumnya terdiri dari bukit dan lembah yang membentuk pola garis dengan arah tertentu. Pola garis tersebut umumnya berakhir pada titik tertentu atau bercabang dan menghubungkan pola garis yang lain. Kombinasi tersebut menghasilkan pola garis sidik jari yang unik pada setiap individu. Proses pengenalan sidik jari dapat dilakukan pada beberapa tingkat detil yang berbeda. Pada tingkat detil yang sederhana, pengenalan sidik jari dilakukan dengan mengklasifikasikan pola garis pada sidik jari tersebut. Sedangkan pada tingkat detil yang lebih spesifik, sidik jari dapat diidentifikasi melalui letak dari titik akhir maupun titik percabangan pola garis pada sidik jari. Pengenalan sidik jari pada tingkat detil ini lebih umum dikenal sebagai deteksi titik minutiae. Lokasi titik minutiae dan arah titik tersebut bersifat unik pada masing-masing individu. Hal inilah yang menjadikan titik minutiae sebagai parameter identifikasi sidik jari yang lebih spesifik.

Isu keamanan data merupakan isu yang sangat krusial dewasa ini. Tindak pencurian data personal seseorang bukan lagi hal baru yang hanya dilakukan oleh segelintir orang atau kelompok tertentu. Umumnya pencurian data tersebut dilakukan

dengan berbagai motif. Mulai dari motif sederhana seperti pencurian data personal untuk keperluan finansial, hingga motif yang bersifat kompleks seperti motif yang berkaitan dengan hal-hal politis. Tak sekedar melakukan pencurian data secara langsung, pihak yang tak bertanggungjawab sering pula mencuri data-data seperti kata kunci atau kode tertentu yang digunakan untuk proses autorisasi. Penggunaan aplikasi pengamanan data seolah tak cukup untuk memberikan rasa aman. Seringkali ditemukan korban pencurian data identifikasi yang tak sadar telah terjadi pencurian kode pengamanan yang dimiliki. Kasus demikian dikenal sebagai *social engineering*, yaitu pemanfaatan terhadap kelengahan pengguna dalam mengamankan kode pengamanan yang dimiliki. Kode pengamanan seperti *Personal Identification Number* (PIN) maupun *password*, memiliki kelemahan yang sulit untuk diatasi dengan teknologi keamanan data yang canggih. PIN maupun password acapkali dibuat menggunakan kombinasi angka, huruf maupun simbol yang membentuk pola tertentu sehingga mudah diingat oleh pengguna. Pada beberapa kasus, seorang pelaku *social engineering* dapat dengan mudah menebak *password* yang dimiliki seseorang. Kemudian, dengan sedikit kreativitas dalam menyusun kombinasi huruf, angka serta simbol yang mungkin digunakan, *password* tersebut dapat dengan mudah berpindah tangan (Pontiroli, 2013).

Beberapa penelitian telah menunjukkan bahwa data biometris seperti sidik jari dapat digunakan untuk mendukung keperluan keamanan data. Selain dapat digunakan sebagai alat bantu otentikasi pengguna, data biometris juga dapat digunakan sebagai kunci dalam proses kriptografi yang bertujuan untuk menyamarkan data. Sehingga data yang diamankan tersebut tidak nampak seperti data berarti. Sifat unik dan universal tersebut yang mendukung penggunaan data biometris untuk keperluan kriptografi data. Sehingga kunci tidak dapat dengan mudah disalahgunakan oleh pihak yang tidak tepat. B. Raja Rao dalam penelitiannya mengungkap bahwa lokasi fitur minutiae pada sidik jari bersifat unik pada tiap individu dan dapat dimanfaatkan untuk membangkitkan kunci kriptografi melalui konkatenasi koordinat minutiae dan sudut arah fitur minutiae tersebut. Lebih jauh lagi, P. Balakumar dan Dr. R. Venkatesan membuktikan bahwa sidik jari juga dapat digabungkan dengan selaput pelangi pada mata untuk menghasilkan kunci yang lebih sulit diduplikasikan. Sedangkan penelitian yang dilakukan oleh Dr. A. Shanmugam dan P. Arul membuktikan bahwa sidik jari bersama standar

keamanan data *Advanced Encryption Standard* (AES) dapat digunakan untuk mengamankan paket data suara pada teknologi VoIP.

Algoritma Rijndael pada AES telah ditetapkan sejak tahun 2002 sebagai standar keamanan data digital. Algoritma tersebut memiliki sifat acak dan difusi yang tinggi. Hal ini didukung oleh pengaplikasian ukuran kunci yang lebih besar dibanding dengan ukuran kunci pada standar keamanan data yang ada sebelumnya. Selain ukuran kunci dan karakter algoritma yang kuat, AES juga menggunakan beberapa mode operasi yang mendukung penggunaannya pada berbagai jenis data. Mode operasi tersebut dirancang sedemikian rupa sehingga AES dapat digunakan secara lebih efektif dan efisien (Sadikin, 2012).

Tugas akhir ini mengaplikasikan fitur minutiae untuk dapat digunakan sebagai pembangkit kunci kriptografi. Memanfaatkan letak ordinat dan sudut orientasi titik minutiae, kunci yang telah dibangkitkan digunakan dalam proses enkripsi dan dekripsi pada berkas audio.

1.2. Rumusan Masalah

Masalah yang dirumuskan dalam topik pembahasan tugas akhir ini adalah implementasi pembangkitan kunci kriptografi menggunakan pola pada sidik jari untuk mengamankan berkas audio dengan format MP3. Standar keamanan data AES digunakan dalam proses kriptografi berkas audio.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam pembahasan tugas akhir ini antara lain :

1. Menghasilkan sebuah sistem aplikasi kriptografi yang memanfaatkan pola unik pada sidik jari untuk membangkitkan kunci kriptografi.
2. Mengimplementasikan proses ekstraksi titik minutiae pada sidik jari.
3. Mengimplementasikan data koordinat dan orientasi pada titik minutiae sebagai pembangkit kunci kriptografi sesuai dengan standar keamanan data yang digunakan.

4. Menguji proses kriptografi pada berkas audio menggunakan kunci yang telah dibangkitkan dari citra sidik jari.

Manfaat yang diharapkan dari penelitian tugas akhir ini adalah untuk mengimplementasikan pola unik pada citra sidik jari sebagai pembangkit kunci kriptografi.

1.4. Ruang Lingkup

Ruang lingkup implementasi citra sidik jari sebagai pembangkit kunci kriptografi adalah sebagai berikut :

1. Citra sidik jari berupa berkas citra dengan format TIFF, BMP, JPEG, dan PNG.
2. Citra yang digunakan merupakan citra sidik jari dari salah satu jari pada tangan manusia.
3. Fitur minutiae pada sidik jari diidentifikasi untuk kemudian diproses lebih lanjut untuk membangkitkan kunci kriptografi.
4. Standar kriptografi yang digunakan pada tugas akhir ini adalah *Advanced Encryption Standard* (AES).
5. Berkas yang digunakan untuk proses kriptografi adalah berkas audio dengan format MP3.
6. Berkas audio yang telah berhasil dienkripsi disimpan sebagai berkas audio berformat MP3 yang tidak dapat diputar ulang.
7. Perangkat lunak dikembangkan pada lingkungan *desktop* menggunakan Microsoft Visual Studio 2010 dengan bahasa pemrograman C#.
8. Tidak dibahas mengenai transmisi data.

1.5. Sistematika Penulisan

Sistematika penulisan pada laporan tugas akhir ini terbagi dalam beberapa pokok bahasan, antara lain :

BAB I PENDAHULUAN

Bab ini memaparkan latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan laporan tugas akhir mengenai Implementasi Pembangkit Kunci Kriptografi berbasis Sidik Jari.

BAB II LANDASAN TEORI

Bab ini memaparkan studi pustaka yang menjadi landasan dalam pengambilan topik tugas akhir. Pada bab ini dibahas mengenai citra digital, sidik jari, pengolahan citra digital, pengenalan pola, kriptografi, algoritma pembangkit kunci kriptografi, rekayasa perangkat lunak, *flowchart*, dan *Unified Modelling Language* (UML).

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi penjelasan mengenai hasil analisa dan perancangan sebelum sistem dikembangkan secara keseluruhan. Mengacu pada model proses yang digunakan, tahap ini meliputi proses komunikasi, perencanaan, dan pemodelan. Bab ini menjabarkan tahap-tahap tersebut dalam bentuk analisa dan rancangan arsitektur sistem dalam bentuk pemodelan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan bagaimana sistem dikembangkan sesuai dengan model proses yang digunakan.

BAB V PENUTUP

Bab penutup berisi kesimpulan akhir dari penelitian serta saran yang dapat dijadikan sebagai acuan dalam pengembangan yang lebih lanjut.