PENERAPAN PENGAMANAN DATA CITRA DIGITAL DENGAN ALGORITMA HILL CIPHER BERBASIS ANDROID

SKRIPSI

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

Disusun Oleh:
ART DWICA WIDHYANATA
24010311130058

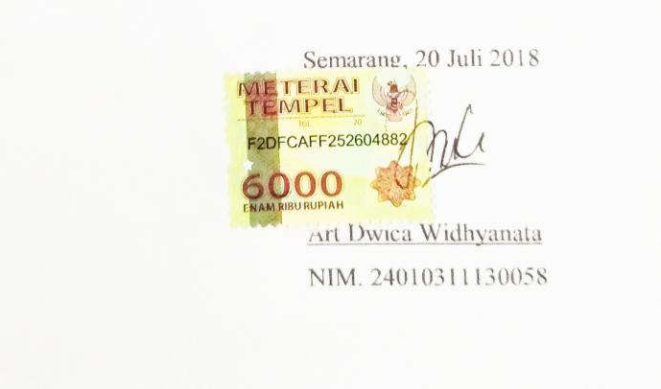
DEPARTEMEN ILMU KOMPUTER/ INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2018

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini,

Nama : Art Dwica Widhyanata
NIM : 24010311130058
Judul : Penerapan Pengamanan Data Citra Digital dengan Algoritma *Hill Cipher* Berbasis Android

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 sepengetahuan 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.



HALAMAN PENGESAHAN

Judul : Penerapan Pengamanan Data Citra Digital dengan Algoritma *Hill Cipher* Berbasis Android

Nama : Art Dwica Widhyanata

NIM : 24010311130058

Telah diujikan pada sidang tugas akhir pada tanggal 28 Juni 2018 dan dinyatakan lulus pada tanggal **28 Juni 2018**

Semarang, 12 Juli 2018

Mengetahui
Ketua Departemen Ilmu Komputer/Informatika
FSM UNDIP

Dr. Retno Kusumaningrum, S.Si., M.Kom.
NIP. 198104202005012001

Panitia Penguji Tugas Akhir
Ketua,

Drs. Suhartono, M.Kom.
NIP. 195504071983031003

HALAMAN PENGESAHAN

Judul : Penerapan Pengamanan Data Citra Digital dengan Algoritma *Hill Cipher* Berbasis Android

Nama : Art Dwica Widhyanata

NIM : 24010311130058

Telah diujikan pada sidang tugas akhir pada tanggal 28 Juni 2018 dan dinyatakan lulus pada tanggal **28 Juni 2018**

Semarang, 12 Juli 2018

Pembimbing

Panji Wisnu Wirawan, S.T., M.T.

NIP. 198104212008121002

ABSTRAK

Kegiatan berkirim pesan atau informasi semakin mudah dan dapat dilakukan dengan berbagai cara seiring dengan perkembangan teknologi, salah satunya menggunakan perangkat *smartphone*. Citra digital merupakan data yang umum untuk dipertukarkan, termasuk data-data yang bersifat rahasia. Oleh karena itu keamanan dan kerahasiaan data citra harus terjaga agar tidak terjadi penyalahgunaan informasi oleh pihak yang tidak berkepentingan. Penelitian tugas akhir ini membahas tentang kriptografi citra digital menggunakan algoritma *Hill Cipher* pada perangkat *smartphone* berbasis Android. Aplikasi ini dapat melakukan proses enkripsi dan dekripsi pada *smarpthone* yang menggunakan sistem operasi Android. Hasil proses aplikasi ini adalah citra acak yang tidak dapat dibaca. Waktu yang dibutuhkan untuk proses enkripsi dan dekripsi bergantung pada dimensi citra yang digunakan. Semakin besar panjang atau lebar suatu citra maka waktu proses semakin lama. Nilai PSNR dari citra asli dan citra hasil dekripsi tinggi karena kualitas kedua citra setara.

Kata kunci: *smartphone,* citra, keamanan, Android, enkripsi, dekripsi, *Hill Cipher*

ABSTRACT

Activities to send messages or information more easily and can be done in various ways along with the development of technology, one of them using smartphone devices. Digital image is common data to be exchanged, including confidential data. Therefore, the security and confidentiality of image data must be maintained in order to avoid misuse of information by unauthorized parties. This research discusses about digital image cryptography using Hill Cipher algorithm on Android-based smartphone device. This application could perform the process of encryption and decryption on smarpthone using the Android operating system. The output of this app was a random image that could not be read. The time required for the encryption and decryption process depended on the image dimension used. The larger the length or width of an image the longer the processing time. The PSNR value of the original image and decrypted image was high because of the equivalent quality of the two images.

Keywords: smartphone, image, security, Android, encryption, decryption, Hill Cipher

KATA PENGANTAR

Segala puji bagi Tuhan Yang Maha Kuasa atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul "Penerapan Pengamanan Data Citra Digital dengan Algoritma *Hill Cipher* Berbasis Android" ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada DepartemenIlmu Komputer/ Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan laporan ini penulis mendapat banyak mendapat bantuan dan dukungan dari berbagai pihak. Untuk itu pada kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada :

1. Dr. Retno Kusumaningrum, S.Si., M.Kom selaku Ketua Departemen Ilmu Komputer / Informatika FSM Universitas Diponegoro.
2. Helmi Arif Wibawa, S.Si, M.Cs selaku Koordinator Tugas Akhir yang membantu dalam proses perizinan tugas akhir.
3. Panji Wisnu Wirawan, S.T., M.T selaku dosen pembimbing yang telah membimbing penulis dalam menyelesaikan tugas akhir ini.
4. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materiataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan. Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya.

Semarang, 28 Juni 2018

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab pendahuluan menjelaskan tentang latar belakang dari pemilihan tema dan judul tugas akhir, rumusan masalah dalam pelaksanaan tugas akhir, tujuan dan manfaat yang dapat diperoleh dari tugas akhir, ruang lingkup yang menjadi batasan tugas akhir, dan sistematika penulisan dokumen tugas akhir ini.

1.1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang sangat pesat memberikan dampak yang besar dalam kehidupan manusia, salah satunya dalam hal pengiriman informasi. Kemajuan teknologi saat ini memungkinkan kegiatan pengiriman informasi atau data dilakukan dengan mudah dan melalui berbagai media, antara lain melalui internet dengan menggunakan fasilitas *e-mail*, transfer data antarperangkat *mobile* (*handphone*, PDA, *flashdisk*), maupun dengan teknologi radio *frequency* (*Bluetooth*, IrDA, GPRS), hingga menggunakan jaringan komputer (Utami & Sukrisno, 2007). Di antara berbagai media tersebut, *smartphone* menjadi salah satu media yang sering digunakan.

Komunikasi dan pertukaran informasi dapat dengan mudah dilakukan secara jarak jauh, seperti antarkota, antarwilayah, antarnegara, bahkan antarbenua. Seiring dengan kemudahan tersebut, tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan melalui *smartphone* semakin meningkat, salah satunya adalah jenis data atau informasi citra digital (Sadikin, 2012). Penggunaan citra digital secara luas di berbagai kegiatan, menuntut keamanan data khususnya untuk data yang bersifat rahasia. Instansi seperti pemerintahan, rumah sakit, militer, perusahaan swasta menggunakan citra digital untuk menyimpan berbagai informasi penting dan kemudian mengirimkan informasi tersebut melalui internet menggunakan *smartphone*. Informasi tersebut misalnya hasil pemeriksaan pasien, pergerakan musuh militer, desain produk baru, foto-foto yang bersifat pribadi, dan lain-lain. Jika informasi tersebut jatuh ke tangan orang yang salah, maka dapat menimbulkan hal-hal yang tidak diinginkan, seperti perang atau penangan pasien yang salah. Hal ini

yang menyebabkan keamanan citra digital menjadi sangat penting (Jayant dan Roy, 2010).

Untuk menjaga kerahasiaan suatu data citra digital, diperlukan cara agar data tersebut tidak bisa dibaca oleh orang yang tidak berkepentingan sehingga informasi tidak tersebar dan terjadi hal-hal yang tidak diinginkan. Salah satu cara dalam meningkatkan kerahasiaan dan keamanan data adalah dengan menyandikan data tersebut. Data yang disandikan diubah bentuknya agar menjadi sulit untuk dipahami maksudnya. Teknik untuk menyandikan data tersebut disebut dengan kriptografi. Kriptografi memegang peranan yang penting dalam menyandikan data, baik data yang bersifat teks maupun digital. Dalam kriptografi, terdapat dua proses utama, yaitu enkripsi dan dekripsi. Enkripsi adalah metode yang digunakan untuk mengodekan data sedemikian rupa sehingga bentuknya berubah dan tidak bisa dipahami isinya. Sedangkan dekripsi adalah kebalikan dari enkripsi, yaitu mengembalikan data yang telah disandikan ke bentuk semula sehingga dapat dimengerti maksud atau isi dari data tersebut. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu kerahasiaan data informasi (*secrecy*) dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan (*authenticity*) (Basuki, 2005).

Dalam kriptografi, teknik penyandian data dibagi menjadi dua, yaitu klasik dan modern. Dalam kriptografi klasik terdapat dua teknik dasar yang digunakan, yaitu teknik substitusi dan teknik transposisi. Teknik substitusi dilakukan dengan mengganti karakter asli dengan karakter lain, sedangkan transposisi dilakukan dengan permutasi karakter. Salah satu algoritma kriptografi klasik adalah *Hill cipher*. *Hill cipher* termasuk algoritma kriptografi klasik yang sulit dipecahkan apabila hanya mengetahui berkas *ciphertext* saja, karena *Hill cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* (Munir, 2006).

Pada penelitian ini, digunakan algoritma *Hill cipher* yang akan diterapkan ke dalam sebuah aplikasi *smartphone* berbasis Android untuk menyandikan suatu berkas citra digital. Aplikasi ini tidak digunakan untuk menyandikan data teks, melainkan hanya untuk menyandikan citra digital saja. Hasil proses dari aplikasi ini adalah berkas citra yang telah terenkripsi, dan dapat dikembalikan ke bentuk semula melalui proses dekripsi.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan, dapat dirumuskan suatu permasalahan, yaitu bagaimana membangun sebuah aplikasi pengamanan citra digital yang memanfaatkan algoritma kriptografi algoritma *Hill cipher* pada *smartphone* Android.

1.3. Tujuan dan Manfaat

Tujuan dilaksanakannya Tugas Akhir ini adalah untuk menerapkan algoritma kriptografi *Hill Cipher* pada pengembangan sebuah aplikasi enkripsi berbasis Android yang digunakan untuk menyandikan citra digital.

Manfaat dari penelitian Tugas Akhir ini adalah untuk meningkatkan keamanan data citra digital yang bersifat penting atau rahasia sehingga tidak disalah gunakan oleh pihak yang tidak bertanggung jawab.

1.4. Ruang Lingkup

Tugas akhir ini memiliki ruang lingkup sebagai batasan-batasan dalam pengerjaannya agar lebih terarah dan tidak keluar dari tujuan yang diharapkan. Batasan-batasan tersebut antara lain:

1. *Input* data berupa teks sebagai kunci dan citra digital sebagai *plainimage.*
2. *Output* berupa citra digital yang telah disandikan dengan format .png.
3. Citra yang digunakan dalam penelitian ini adalah citra berekstensi .png.
4. Aplikasi hanya mengenkripsi dan mendekripsi *file* citra digital, tidak dapat mengenkripsi atau mendekripsi teks.
5. Algoritma kriptografi yang digunakan adalah algoritma *Hill cipher* dengan matriks kunci berordo 3x3.
6. Kunci enkripsi yang digunakan berupa susunan huruf kecil dari a sampai dengan z dengan panjang 9 karakter.
7. Sistem operasi *mobile* yang digunakan dalam pengembangan aplikasi ini adalah Google® Android versi 7.0 dengan sistem operasi minimum yang dapat dites adalah Android versi 5.0

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang hal-hal yang melatar belakangi dari pembuatan tugas akhir ini, rumusan permasalahan yang dikerjakan, tujuan dan manfaat yang diharapkan, ruang lingkup yang membatasi, dan sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Bab tinjauan pustaka menjelaskan tentang istilah-istilah dan metode-metode yang digunakan di dalam penulisan tugas akhir ini.

BAB III DEFINISI KEBUTUHAN, ANALISIS, DAN PERANCANGAN

Bab definisi kebutuhan, analisis dan perancangan sistem ini menjelaskan tentang definisi kebutuhan, analisa dan perancangan sistem yang akan dibuat dan dikembangkan oleh penulis.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan tentang implementasi sistem yang dibangun berdasarkan perancangan yang sudah dijelaskan pada bab sebelumnya, beserta hasil pengujian dari sistem yang dibuat.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dari pengerjaan tugas akhir ini, beserta dengan saran yang dapat diajukan guna pengembangan sistem ini ke depannya.