APLIKASI KEAMANAN CITRA DIGITAL PADA PERANGKAT BERBASIS ANDROID MENGGUNAKAN TRANSFORMASI *DISCRETE COSINE TRANSFORM*, KRIPTOGRAFI *TWOFISH*, DAN ALGORITMA *FISHER YATES SHUFFLING*

SKRIPSI

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

Disusun oleh:
Ardhan Fajriansyah
24010310141021

DEPARTEMEN ILMU KOMPUTER/INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2016

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	:	Ardhan Fajriansyah
NIM	:	24010310141021
Jurusan	:	S-1 Teknik Informatika
Judul Skripsi	:	APLIKASI KEAMANAN CITRA DIGITAL PADA PERANGKAT BERBASIS ANDROID MENGGUNAKAN TRANSFORMASI *DISCRETE COSINE TRANSFORM*, KRIPTOGRAFI *TWOFISH*, DAN ALGORITMA *FISHER YATES SHUFFLING*

Dengan ini saya menyatakan bahwa tugas akhir/skripsi ini adalah hasil pekerjaan saya sendiri. Sepanjang pengetahuan saya, dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar kesarjanaan serta 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

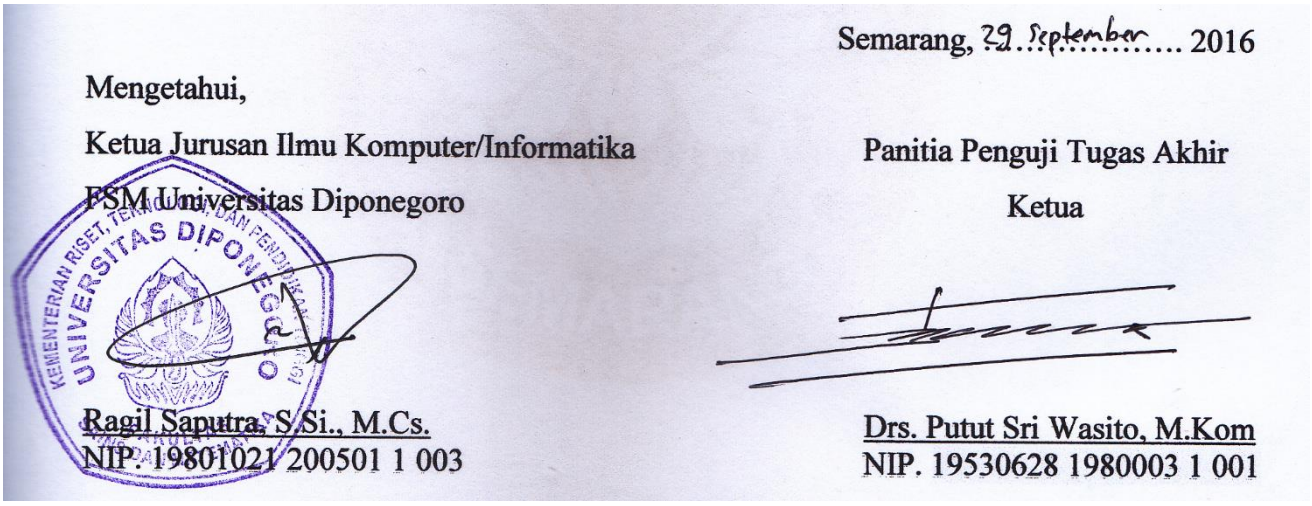
Judul : Aplikasi Keamanan Citra Digital pada Perangkat Berbasis Android Menggunakan Transformasi *Discrete Cosine Transform*, Kriptografi *Twofish*, dan Algoritma *Fisher Yates Shuffling*

Nama : Ardhan Fajriansyah

NIM : 24010310141021

Jurusan : S-1 Teknik Informatika

Telah diujikan pada sidang tugas akhir pada tanggal ……. 2016 dan dinyatakan lulus pada tanggal ……. **2016**.



Semarang, 29 September 2016

Mengetahui,
Ketua Jurusan Ilmu Komputer/Informatika
FSM Universitas Diponegoro

Ragil Saputra, S.Si., M.Cs.
NIP. 19801021 200501 1 003

Panitia Penguji Tugas Akhir
Ketua

Drs. Putut Sri Wasito, M.Kom
NIP. 19530628 1980003 1 001

HALAMAN PENGESAHAN

Judul : Aplikasi Keamanan Citra Digital pada Perangkat Berbasis Android Menggunakan Transformasi *Discrete Cosine Transform*, Kriptografi *Twofish*, dan Algoritma *Fisher Yates Shuffling*

Nama : Ardhan Fajriansyah

NIM : 24010310141021

Jurusan : S-1 Teknik Informatika

Telah diujikan pada sidang tugas akhir pada tanggal ……. 2016.

Semarang, 29 September 2016

Pembimbing

Helmie Arif Wibawa, S.Si, M.Cs
NIP. 19780516 200312 1 001

ABSTRAK

Penggunaan media penyimpanan pada telepon seluler merupakan hal yang umum pada saat ini. Segala macam data digital dapat dengan mudah disimpan pada telepon seluler, salah satunya yaitu gambar. Gambar merupakan data yang bersifat informatif, bahkan terkadang mengandung hal yang sensitif bagi sebagian orang. Kurangnya keamanan dalam menyimpan gambar pada telepon seluler dapat menyebabkan berbagai permasalahan, contohnya penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu dibutuhkan suatu metode untuk mengatasi masalah tersebut. Pada penelitian kali ini akan dibahas tentang pembuatan aplikasi *mobile* berbasis Android yang dapat melakukan proses enkripsi dekripsi dengan mengacak *bitmap color* suatu citra. Metode yang digunakan adalah *Discrete Cosine Transform* (DCT) untuk mentransformasi citra asli dari domain spasial ke dalam domain frekuensi pada ruang warna RGB ditambah dengan metode kriptografi *Twofish* untuk pembangkitan kunci yang kemudian digabungkan dengan proses pengacakan algoritma *Fisher Yates Shuffling*.

Kata kunci: Gambar, Android, Enkripsi, Dekripsi, *Discrete Cosine Transform*, RGB, *Twofish*, *Fisher Yates Shuffling*.

ABSTRACT

The use of the storage media on mobile phones are commonly known at this time. All kinds of digital data can be easily stored on the mobile phone, one of which is an image. Images are an informative data that sometimes even contains a sensitive issue for some people. Lack of security in storing the images on mobile phones can cause various problems, such misuse of information by parties who are not responsible. Therefore, there need a method to resolve this issue. In this research will be discussed about the creation of Android-based mobile application that can perform encryption decryption process to randomize the bitmap color of an image. The method that is used in this research is the Discrete Cosine Transform (DCT) to transform the original image from the spatial domain into the frequency domain in the RGB color space, coupled with Twofish methods for generate the key then combined with the process of randomization algorithm Fisher Yates Shuffling.

Keywords: Image, Android, Encryption, Decryption, Discrete Cosine Transform, RGB, *Twofish*, *Fisher Yates Shuffling*.

KATA PENGANTAR

Segala Puji bagi Tuhan Yang Maha Esa atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul "Aplikasi Keamanan Citra Digital pada Perangkat Berbasis Android Menggunakan Transformasi *Discrete Cosine Transform*, Kriptografi *Twofish*, dan Algoritma *Fisher Yates Shuffling*" ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer/ Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

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

1. Ragil Saputra, S.Si, M.Cs. selaku Ketua Jurusan Ilmu Komputer / Informatika FSM Universitas Diponegoro.
2. Helmie Arif Wibawa, S.Si, M.Cs. selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika FSM Universitas Diponegoro sekaligus selaku dosen Pembimbing.
3. 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 materi ataupun 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, 2016

Penulis

DAFTAR ISI

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup serta sistematika penulisan penelitian mengenai pembuatan aplikasi keamanan digital pada perangkat berbasis Android dengan menggabungkan metode transformasi citra *Discrete Cosine Transform*, kriptografi algoritma *Twofish*, dan pengacakan *Fisher Yates Shuffling*.

1.1. Latar Belakang

Di era globalisasi saat ini, informasi berkembang semakin pesat. Selain komputer, penggunaan *smartphone* sudah menjadi kebutuhan sekunder di kalangan masyarakat. Di balik penggunaan *smartphone* terdapat sekian banyak sistem operasi yang memiliki ragam dan fitur tersendiri. Android merupakan salah satu sistem operasi yang tengah berkembang dan memiliki daya tarik bagi penggunanya sehingga tidak heran sistem operasi Android menjadi pilihan utama bagi para pengguna *smartphone*.

Tingginya tingkat pengguna *smartphone* membawa pengaruh besar terhadap keamanan informasi yang terdapat di dalamnya. Dimana penggunaan *smartphone* sebagai media penyimpanan maupun pertukaran informasi. Apabila informasi ini diambil, diketahui, bahkan dimanipulasi oleh pihak-pihak yang tidak berhak atas informasi tersebut tentu menjadi hal yang sangat merugikan bagi penggunanya. Salah satu contoh informasi yang bersifat pribadi adalah *file* gambar, pemilik informasi harus yakin bahwa *file* gambar tersebut aman apabila *smartphone* secara tidak dikehendaki berpindah tangan, pemilik tidak perlu khawatir informasi pribadi yang dimilikinya disalahgunakan sehingga informasi yang tersimpan dapat tetap aman dan terjaga keasliannya.

Salah satu solusi yang ditawarkan untuk menjawab permasalahan proteksi visual pada citra adalah dengan menyamarkan *file* tersebut menjadi suatu objek yang tidak jelas agar tidak mudah untuk dimengerti dan tetap terjaga kerahasiaannya. Hal ini dapat dilakukan dengan menggabungkan beberapa metode, yaitu metode transformasi DCT (*Discrete Cosine Transform*), penyandian kunci menggunakan kriptografi

algoritma Twofish, dan teknik pengacakan citra berdasarkan metode *Fisher Yates Shuffling*.

Metode DCT adalah transformasi matematika yang mengubah data citra dari domain spasial ke domain frekeunsi. Frekuensi inilah yang disebut dengan koefisisen DCT, yang mana nantinya akan dilakukan proses pengacakan. Hasil transformasi balik ke domain spasial akan menghasilkan *cipher-image* yang berbeda dan memiliki karakteristik yang tidak sama dengan *plain-image* (Rinaldi, 2012). Metode transformasi DCT digunakan dengan tujuan untuk menambah tingkat kerumitan proses penyandian citra.

Sementara teknik pengacakan citra pada aplikasi ini menggunakan metode *Fisher Yates Shuffling*. Metode *Fisher Yates* mengacak urutan citra berdasarkan *seed* (nilai awal) yang ditentukan dari hasil enkripsi kunci khusus. Proses pembangkitan kunci itu sendiri menggunakan teknik kriptografi algoritma *Twofish*. Pengunaan kriptografi sebagai alat keamanan citra bukan merupakan hal yang baru, karena sebelumnya telah banyak dilakukan penelitian yang mengangkat kajian tersebut namun dengan beberapa macam metode yang berbeda. Sebelumnya telah dilakukan penelitian yang menghasilkan sebuah aplikasi keamanan citra menggunakan kriptografi algoritma AES Rijndael dengan kombinasi transformasi DWT (Bagus S.W.P., 2010).

Oleh karena itu, pada penelitian kali ini akan dibangun suatu aplikasi keamanan citra pada perangkat berbasis sistem operasi Android dengan menggabungkan ketiga metode tersebut yaitu transformasi *Discrete Cosine Transform*, kriptografi algoritma *Twofish*, dan pengacakan *Fisher Yates Shuffling* yang diharapkan dapat menjadi salah satu sistem keamanan citra yang efektif.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana merancang dan membangun aplikasi pada *smartphone* berbasis sistem operasi Android dengan menggabungkan beberapa metode yaitu transformasi *Discrete Cosine Transform*, kriptografi algoritma *Twofish*, dan pengacakan *Fisher Yates Shuffling*.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari penulisan ini adalah untuk menghasilkan suatu aplikasi keamanan citra digital pada perangkat berbasis sistem operasi Android yang mengimplementasikan DCT untuk transformasinya, *Fisher Yates* untuk proses pengacakan citra, dan algoritma *Twofish* untuk penyandian kuncinya.

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Sebagai media untuk peng-implementasian ilmu pengetahuan teknologi pada bidang keamanan data.
2. Dapat menambah ilmu mengenai sistem operasi Android serta bahasa pemrograman yang digunakan dalam pembuatan aplikasi.
3. Mendapatkan wawasan mengenai transformasi DCT, kriptografi *Twofish*, dan *Fisher Yates Shuffling* dalam proses peng-implementasiannya.
4. Membantu meningkatkan keamanan di dunia teknologi dan informasi terutama mengenai keamanan dalam proses menyimpan, mengirim, maupun menerima informasi menggunakan perangkat bergerak berbasis sistem operasi Android.

1.4. Ruang Lingkup

Dalam penyusunan tugas akhir ini diberikan ruang lingkup yang jelas agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan.

1. Input berupa citra diam dengan format PNG.
2. Menggunakan bahasa pemrograman Java dengan *development tools* Android Studio.
3. Pada proses transformasi menggunakan teknik *Discrete Cosine Transform*.
4. Proses penyandian kunci menggunakan kriptografi algoritma *Twofish*.
5. Proses *shuffling* dan *unshuffling* dengan metode *Fisher Yates*.
6. Proses *input* dan *output* hanya bisa dilakukan dalam satu perangkat.
7. Untuk mengetahui perbandingan kualitas citra asli dengan citra hasil rekayasa adalah dengan menghitung nilai PSNR-nya.

1.5. Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup serta sistematika penulisan penelitian tugas akhir mengenai pembuatan aplikasi keamanan digital pada perangkat berbasis Android dengan menggabungkan metode transformasi citra *Discrete Cosine Transform*, kriptografi algoritma *Twofish*, dan pengacakan *Fisher Yates Shuffling*.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori yang digunakan dalam penyusunan tugas akhir ini. Teori yang digunakan pada penyusunan tugas akhir ini meliputi pengertian citra digital, *Disrete Cosine Transformation*, *Twofish*, *Fisher Yates Shuffling, Peak Signal to Noise Ratio* (PSNR), proses pengembangan perangkat lunak, permodelan fungsional dan pengujian perangkat lunak.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang analisis masalah dan rancangan penyelesaiannya. Bab ini berisi antara lain rancangan perhitungan dan solusi permasalahan, gambaran arsitektur aplikasi, rancangan alur program dalam bentuk *flowchart* serta rancangan antar muka.

BAB IV PERANCANGAN DAN ANALISA

Bab ini menguraikan implementsi algoritma dan antarmuka yang telah dirancang serta langkah-langkah pengujiannya. Bab ini juga membahas tentang analisis hasil dari penelitian tugas akhir ini.

BAB V PENUTUP

Penutup berisi kesimpulan dari pengerjaan penelitian tugas akhir ini dan saran-saran dari penulis untuk pengembangan lebih lanjut dari penelitian serupa.