**Progresif:** Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

# Perancangan Aplikasi Steganografi Menggunakan Metode *Discrete Cosine Transformation* berbasis Android

**Saifuddin[1]*, Agus Rakhmadi Mido[2], E.I.H. Ujianto[3]**
[1,2,3]Program Studi Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
[1,2,3]Jl. Siliwangi (Ringroad Utara), Jombor, Sleman, D.I. Yogyakarta 55285
[2]agus.rakhmadi.mido@student.uty.ac.id, [3]erik.iman@uty.ac.id
**Corresponding Author*: saifuddin@student.uty.ac.id

**ABSTRAK**

Dalam era perkembangan teknologi digital sekarang pengiriman data berupa digital lebih cepat dan mudah, namun dalam pendistribusian data digital melalui jaringan publik seperti internet tidak cukup aman karena sering terjadi pelanggaran hak cipta, pemalsuan, pembajakan, dan penipuan. Oleh karena itu, metode untuk melindungi data digital terutama data yang sensitif sangat diperlukan. Meskipun penggunaan dokumen elektronik sudah menjadi hal yang umum, tidak banyak orang dapat mengenali dokumen-dokumen yang berisi data tersembunyi. Didalam steganografi, kita bisa menyembunyikan sebuah pesan, gambar, maupun file kedalam sebuah gambar, video, maupun audio. Didalam steganografi, terdapat proses penyisipan bit-bit pesan kedalam bit-bit penampung pada tiap-tiap pixel citra. Dilakukan juga pengujian terhadap citra stego dengan menggunakan *mean square error* (MSE) dan *peak signal to noise ratio* (PSNR). Berdasarkan pengujian menggunakan algoritma MSE menghasilkan nilai rata-rata sebesar 0.472 dan pengujian menggunakan algoritma PSNR menghasilkan nilai rata-rata sebesar 54.356 dB.

***Kata kunci:*** *Aplikasi Steganografi, Metode Discrete Cosine Transformation, Berbasis Android, Mean Square Error, Peak Signal to Noise Ratio*

***ABSTRACT***

*In the era of digital technology development, digital data transfer is faster and easier, but in the distribution of digital data through public networks such as the internet is not safe enough because there are often copyright violations, counterfeiting, piracy, and fraud. Therefore, methods to protect digital data, especially sensitive data, are needed. Although the use of electronic documents has become common, not many people can recognize documents that contain hidden data. In steganography, we can hide a message, image, or file into an image, video or audio. In steganography, there is the process of inserting message bits into storage bits at each pixel of the image. A stego image was also tested using mean square error (MSE) and peak signal to noise ratio (PSNR). Based on testing using the MSE algorithm produces an average value of 0.472 and testing using the PSNR algorithm produces an average value of 54,356 dB.*

***Keywords****: Application of Steganography, Discrete Cosine Transformation Method, Based on Android, Mean Square Error, Peak Signal to Noise Ratio*

## 1. Pendahuluan

Dalam era perkembangan teknologi digital sekarang pengiriman data berupa digital lebih cepat dan mudah, namun dalam pendistribusian data digital melalui jaringan publik seperti internet tidak cukup aman karena sering terjadi pelanggaran hak cipta, pemalsuan, pembajakan, dan penipuan. Oleh karena itu, metode untuk melindungi data digital terutama data yang sensitif sangat diperlukan. Meskipun penggunaan dokumen elektronik sudah menjadi hal yang umum, tidak banyak orang dapat mengenali dokumen-dokumen yang berisi data tersembunyi. Dikatakan tersembunyi karena data biasanya terdapat di dalam sebuah berkas, tetapi sulit untuk diidentifikasi keberadaannya. Data tersembunyi dapat diklasifikasikan menjadi

dua jenis, yang dibuat secara otomatis oleh aplikasi dan yang dibuat dan disembunyikan oleh seseorang untuk tujuan tertentu. Para peretas bisa melakukan berbagai macam hal termasuk penyadapan informasi yang bisa sangat merugikan bagi korbanya, sehingga banyak sekali berbagai macam upaya untuk melakukan mencegahan berbagai macam serangan peretas, diantaranya adalah kriptografi. Dalam perkembangannya ada beberapa munculah sebuah metode yang bisa di bilang lebih aman di banding kriptografi, yang sering disebut dengan steganografi. Didalam steganografi, kita bisa menyembunyikan sebuah pesan, gambar, maupun file kedalam sebuah gambar, video, maupun audio. Didalam steganografi, terdapat proses penyisipan bit-bit pesan kedalam bit-bit penampung pada tiap-tiap pixel citra. Dalam penelitian yang terkait steganografi adalah metode yang dapat menempatkan data ke media tanpa dampak nyata pada sampul media. Selain itu, data tersembunyi dapat diekstraksi dengan perbedaan minimal. Dalam tulisan ini, dua dimensi transformasi wavelet diskrit digunakan untuk steganografi dalam gambar warna 24-bit. Sub-band ini diperoleh oleh 3 tingkat menerapkan *Discrete Wavelet Transform* (DWT). Juga untuk meningkatkan ketahanan steganografi terhadap penanaman atau penyisipan tanda air terlihat, dua saluran gambar warna digunakan secara bersamaan. Untuk meningkatkan keamanan, gambar yang diekstraksi Kesamaan juga diukur dengan koefisien korelasi dua dimensi dengan kemiripan lebih dari 99%. Selain itu, resistensi steganografi terhadap peningkatan dan penurunan kecerahan dan kontras, lossy kompresi, memotong gambar, mengubah skala dan menambahkan noise dapat diterima [1]. Dalam penelitian lain telah menggunakan embedding *Least Significant Bit* (LSB) bersama dengan F5 dan embedding matriks pada gambar untuk mendapatkan keamanan stego-image. Menunjukkan bahwa MSE & PSNR dari teknik LSB yang mana matrix embedding menghasilkan lebih baik. Algoritma ini dapat diterapkan untuk skala abu-abu 8 bit, 24 bit, dan gambar berwarna. Kami telah menggunakan matriks embedding dengan kode hamming biner untuk mendapatkan efisiensi embedding yang lebih baik yang masih dapat ditingkatkan dengan yang lain kode juga [2]. Teknik menggabungkan steganograpi dan kriptograpi visual akan memaksimalkan keamanan transaksi online antara penjual dan pembeli. Sehingga dapat mengurangi resiko shipping dan pencurian data bank pengguna/pembeli [3]. Metode steganografi yang diusulkan yang dijelaskan dalam makalah ini membantu berhasil menyembunyikan gambar rahasia ke dalam gambar sampul, dengan distorsi minimum yang dibuat untuk gambar sampul. Pertama, gambar diacak menggunakan algoritma Arnold dan disematkan ke gambar sampul dengan menggunakan algoritma LSB. Hasil pengujian menunjukkan tingkat keberhasilan steganografi video dengan menggunakan metode LSB adalah 38%, metode *discrete cosine transformation* (DCT) adalah 90%, dan gabungan metode LSB-DCT adalah 64%, sedangkan hasil perhitungan MSE, nilai MSE metode DCT paling rendah dibandingkan metode LSB dan gabungan metode LSB-DCT[4].

## 2. Tinjauan Pustaka

### 2.1 Analisis GAP

Dari studi beberapa algoritma steganografi, itu mengamati bahwa domain transformasi memiliki kemampuan untuk memegang pesan rahasia setelah menerapkan proses pengolahan gambar tersebut seperti mengubah ukuran, memotong, memutar dll. Sekali lagi, dapat disimpulkan bahkan sebelum memaksakan algoritma embedding, penggunaan algoritma kriptografi akan memberikan tingkat yang lebih baik keamanan [5]. Di kasus gambar berwarna, IWT diambil untuk setiap saluran, tanda tangan pemancar dan panjangnya teks rahasia disembunyikan dalam koefisien aproksimasi komponen merah dari gambar warna, teks rahasia itu sendiri disembunyikan di koefisien aproksimasi dari kedua hijau dan komponen biru, dan IWT terbalik diambil. Selanjutnya, algoritma yang diusulkan mengekstrak data tersembunyi efisien tanpa menggunakan gambar sampul asli. Eksperimental hasil membuktikan bahwa algoritma yang diusulkan dapat menanamkan teks rahasia yang lebih besar (hingga 8 192 digit dalam kasus ini) gambar skala abu-abu dan 24 576 digit dalam hal warna gambar dengan hasil PSNR dan NCC yang lebih baik [6]. Metode pengukuran yang digunakan untuk menentukan kualitas gambar stego adalah sinyal puncak ke rasio noise (PSNR) dan korelasi silang dinormalisasi (NCC) untuk mengukur kualitas ekstraksi pesan yang didekripsi [7]. Implementasi otentikasi multi-party key dan steganografi untuk transaksi data dengan beberapa pengguna, dalam informasi yang akan disimpan didalam cloud akan terenkripsi menggunakan metode steganography sehingga menjamin keamanan data pengguna [8]. Sistem implementasi teknik steganografi dengan metode AMELSBR dan DCT ini dapat digunakan dengan baik untuk

menyembunyikan berkas di dalam media penampung gambar dan dapat memberikan keamanan dalam pengiriman data. Ketahanan gambar pada manipulasi seperti *brightness, contrast*, dan *cropping* ditentukan oleh komposisi warna, metode yang dipakai, dan ukuran gambar. Tidak terlihat perbedaan yang signifikan pada gambar dikarenakan penggunaan format file gambar (.png) sebagai input dan output. Dengan demikian format file (.png) tersebut baik digunakan untuk teknik steganografi [9]. Keamanan data dengan penyisipan pesan pada suatu media gambar atau steganografi, penelitian sebelumnya masih banyak penyisipan pesan berupa text kalimat saja dan beberapa menggunakan file berformat txt.

Penelitian saat ini isi pesan dapat berupa beberapa file penting yang memiliki format extension bermacam-macam seperti doc, docx, pdf, file terkompres seperti rar. Isi dari setiap file juga ada yang *text* saja dan ada juga campuran dengan gambar dan rumus dan semuanya memili kapasitas berbeda-beda, maka pada penelitian ini merealisasikan penyisipan pesan dengan teknik steganografi dengan metode *discrete cosine transformation* (DCT) yang dilakukan pada citra yang diproses interpolasi bilinear terlebih dahulu [10]. Implementasi pada sistem yang dibangun dilakukan dengan menyandikan pesan pada penerapan metode steganografi citra dalam menyembunyikan pesan tersandi yang dihasilkan ke dalam sebuah citra warna (RGB) dalam domain Discrete Cosine Transform dengan teknik penyisipan Spread Spectrum [11]. Kapasitas pesan pada steganografi DCT sekuensial lebih besar dibandingkan dengan steganografi DCT F5 baik sebelum penerapan POIE maupun setelah penerapan POIE, kualitas citra stego pada steganografi DCT F5 lebih baik dibandingkan dengan steganografi DCT sekuensial baik sebelum penerapan POIE maupun setelah penerapan POIE, baik steganografi DCT F5 maupun steganografi DCT sekuensial sama-sama tidak memiliki ketahanan terhadap manipulasi terhadap citra stego [12]. Penelitian ini menghasilkan kombinasi teknik steganografi dan kriptografi dengan metode LSB–RSA. RSA merupakan teknik kriptografi yang populer dapat diterapkan pada citra digital [13].

### 2.2 Pengertian *Discrete Cosine Transformation* (DCT)

DCT memisahkan gambar menjadi sub-domain spektral dengan tujuan yang berbeda dan sehubungan dengan kualitas visual gambar. Kompresi JPEG menggunakan DCT dalam blok 8 × 8. Persamaan umum untuk DCT 2D (8 × 8 item data) didefinisikan oleh persamaan 1 dan 2.

1) Forward DCT

$$S_{vu} = \frac{1}{4} C_u C_v \sum_{x=0}^{7} \sum_{y=0}^{7} s_{yx} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16} \quad (1)$$

2) Inverse DCT

$$s_{yx} = \frac{1}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} C_u C_v S_{vu} \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16} \quad (2)$$

Blok 8 × 8 sampel gambar sumber secara efektif berukuran x dan y. FDCT mengambil sinyal seperti input dan menguraikannya menjadi 64 sinyal basis ortogonal. *Output* dari FDCT terdiri dari tiga komponen frekuensi: rendah, sedang dan tinggi. Komponen frekuensi terendah (dengan frekuensi nol) dikenal sebagai koefisien DC dan 63 lainnya sebagai koefisien AC. Visualisasi dari blok data setelah DCT digambarkan pada Gambar 1.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DC | 1 | 5 | 6 | 14 | 15 | 27 | 28 |
| 2 | 4 | 7 | 13 | 16 | 26 | 29 | 42 |
| 3 | 8 | 12 | 17 | 25 | 30 | 41 | 43 |
| 9 | 11 | 18 | 24 | 31 | 40 | 44 | 53 |
| 10 | 19 | 23 | 32 | 39 | 45 | 52 | 54 |
| 20 | 22 | 33 | 38 | 46 | 51 | 55 | 60 |
| 21 | 34 | 37 | 47 | 50 | 56 | 59 | 61 |
| 35 | 36 | 48 | 49 | 57 | 58 | 62 | 63 |

Gambar 1. Distribusi Frekuensi blok 8x8 DCT

Pada gambar 1, Komponen berwarna putih adalah komponen frekuensi rendah, abu-abu adalah komponen frekuensi menengah, dan yang berwarna hitam adalah komponen frekuensi tinggi. Citra (*image*) adalah gambar pada bidang dua dimensi. Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (continue) dari intensitas cahaya pada bidang dua dimensi. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut [14]. Citra (image) adalah kombinasi antara titik, garis, bidang dan warna untuk menciptakan suatu imitasi dari suatu objek, biasanya objek fisik atau manusia. Citra bisa berwujud gambar (picture) dua dimensi seperti lukisan, foto, dan yang berwujud tiga dimensi seperti, patung(14). Adapun format file gambar yaitu bitmap, JPEG, dan PNG.

Bitmap (BMP) merupakan format citra yang baku dilingkungan sistem Microsoft Windows dan IBM OS/2. Kualitas BMP lebih baik dan dengan ukuran yang lebih baik dari format JPG/ JPEG dan GIF. Format file Bitmap versi baru dari Microsoft Windows, setiap berkas/file terdiri dari header file, header bitmap, informasi palet, dan data bitmap.

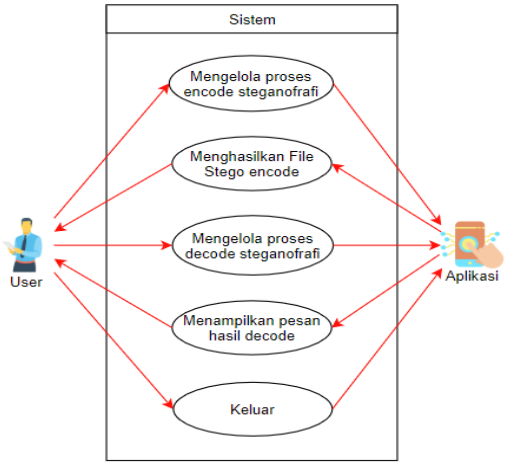
*Joint Photographic Experts Group* (JPEG) dikembangkan oleh para ahli fotografi untuk mendapatkan gambar yang berukuran rasional tapi tetap menyimpan persepsi gambar yang baik. Bersifat lossy dengan tingkat lossness yang dapat diatur. Bagus untuk mengkompresi foto-foto natural tetapi kurang cocok untuk computer-generated images (CGI).

*Portable Graphics Network* (PNG) digunakan di internet dan merupakan format penggati GIF, setelah GIF terkena patent LZW yang dilakukan oleh Unisys. Diprakarsai oleh Thomas Boutell dari PNG Development Group, dan versi finalnya di-release pada 1 Oktober 1996. Memiliki kedalaman warna 48-bit. Hasil pengujian menunjukkan tingkat keberhasilan steganografi video dengan menggunakan metode LSB adalah 38%, metode DCT adalah 90%, dan gabungan metode LSB-DCT adalah 64%. Sedangkan hasil perhitungan MSE, nilai MSE metode DCT paling rendah dibandingkan metode LSB dan gabungan metode LSB-DCT [15]. Penelitian memberikan kontribusi untuk memperbesar kapasitas penyisipan sebagai daya tampung dengan menggunakan teknik penggabungan antara teknik metode DCT dan interpolasi bilinear. Hasil dari penelitian memiliki barbagai kombinasi hasil uji beberapa standar hasil pengujian performansi pada uji Imperectibility berhasil diekstrak, Fidelity berhasil diekstrak, Robustness gagal diekstrak dan Recovery berhasil diekstrak. Keberhasilan dalam kategori kurang baik, karena mendapatkan tingkat akurasi dengan MSE senilai 8.35 namun nilai PSNR sebesar 27.87 dB [16].

## 3. Metodologi

### 3.1 Perancangan Aplikasi

Menyembunyikan pesan pada citra digital ini menggunakan metode discrete cosine transform. Metode ini dapat digunakan untuk menyisipkan pesan dan dapat diterima oleh penerima dengan menggunakan kata sandi yang telah dimasukkan pengirim. Adapun perancangan fungsi pada aplikasi yang dibuat digambarkan pada Gambar 2.



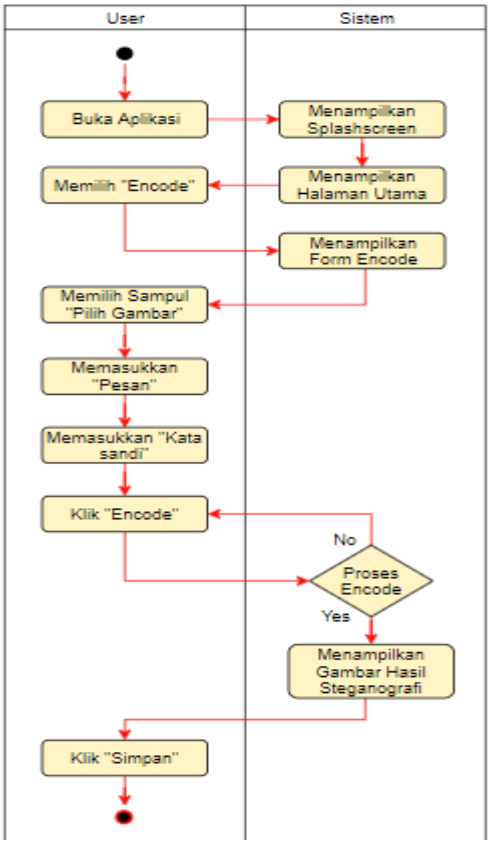

Gambar 2. Perancangan Fungsi Aplikasi

Pada gambar 2, dijelaskan bahwa user dapat menggunakan fungsi aplikasi dan peran aplikasi akan merespon tiap fungsi yang diinginkan user. Perancangan aplikasi memiliki dua fungsi

utama yaitu fungsi encode atau penyisipan pesan kedalam citra digital. Proses encode pada aplikasi steganografi ini adalah sebagai berikut:

1. Pilih gambar yang akan dijadikan *cover*
2. Masukkan pesan rahasia yang akan disisipkan.
3. Memasukkan kata sandi
4. Sistem melakukan proses penyisipan pesan rahasia kedalam *cover* menggunakan metode DCT
5. Jika berhasil, sistem akan menampilkan gambar baru hasil dari proses encode. Jika tidak berhasil, sistem akan meminta gambar lainnya.
6. Unduh gambar untuk menyimpan

Berikut adalah *flowchart* pada proses encode pesan, dapat dilihat pada gambar 3.



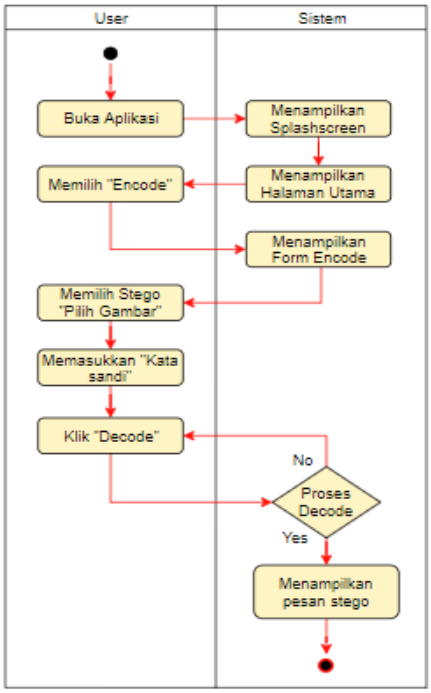

Gambar 3. Diagram Penyisipan Pesan

Pada gambar 3 aplikasi akan menampilkan halaman *splash screen* dalam beberapa detik dan akan dialihkan ke halaman utama aplikasi. Pada halaman utama aplikasi mempunyai menu utama yaitu encode dan decode. Perancangan dalam proses encode memiliki formulir yang harus diisi untuk mendapatkan hasil dari steganografi. Dimulai dengan memilih gambar sebagai sampul, memasukkan pesan teks atau pesan rahasia, dan memasukkan kata sandi untuk keperluan decode penerima, jika salah satu form tidak terisi proses encode tidak bias digunakan. Setelah proses encode selesai, akan ditampilkan hasil citra digital yang telah disisipkan pesan rahasia dan dapat disimpan ke dalam folder *download* pada *storage smartphone.*

Untuk perancangan proses *decode* pada aplikasi steganografi ini adalah sebagai berikut:

1. Masukan citra yang mengandung pesan (*stego-Image*)
2. Memasukkan kata sandi
3. Sistem melakukan proses decode stego image menggunakan metode DCT
4. Jika berhasil, sistem akan menampilkan pesan rahasia hasil dari proses decode. Jika tidak berhasil, sistem akan memberitahukan pesan *error*.

Berikut adalah *flowchart* pada proses encode pesan, dapat dilihat pada gambar 4.




Gambar 4. Diagram Ekstrak Citra

Pada Gambar 4, fungsi decode yang akan berguna untuk ekstrak file yang telah disisipkan pesan dengan menggunakan kata sandi yang digunakan. Pada halaman decode juga terdapat formulir yang harus diisi untuk melakukan proses decode citra. Dimulai dengan memilih file citra yang telah di encode, memasukkan kata sandi. Kemudia decode dapat dilakukan. Jika kata sandi benar akan ditampilkan pesan rahasia.

### 3.2 Pengujian Aplikasi

Pengujian aplikasi steganografi dilakukan untuk mengetahui fungsi-fungsi yang terdapat pada aplikasi steganografi. Aplikasi dengan menggunakan algoritma DCT dalam menyembunyikan pesan rahasia kedalam citra digital. Aplikasi mempunyai fungsi utama yaitu sistem *encoding* dan sistem *decoding.* Adapun alur sistem encode sebagai berikut: 1) Memilih menu encode; 2) Memilih citra digital; 3) Memasukkan pesan rahasia; 4) Memasukkan *key* atau kata sandi; 5) Lakukan proses encode; 6) Mengunduh hasil citra stego

Pada sistem decode dilakukan untuk mengembalikan pesan rahasia yang telah disisipkan didalam citra stego. Adapun alur sistem decode sebagai berikut: 1) Memilih menu decode; 2) Memilih citra stego; 3) Memasukkan key atau kata sandi citra stego; 4) Lakukan proses decode

Proses decode dikatakan berhasil jika sistem dapat mengebalikan pesan rahasia yang telah disisipkan. Tetapi, beberapa kemungkinan proses decode gagal diantaranya citra yang dipilih bukan citra stego atau key atau kata sandi salah.

Penelitian ini menggunakan pengujian *Peak Signal to Noise Ratio* (PNSR) dan *Mean Square Error* (MSE). PSNR digunakan untuk menentukan kualitas gambar setelah disisipi pesan. Citra stego dibandingkan dengan citra asli untuk menentukan kualitas citra. Semakin besar nilai PSNR berarti penyisipan pesan ke dalam citra asli tidak menyebabkan penurunan kualitas gambar stego. Sebaliknya jika nilai PSNR semakin kecil maka pada gambar stego akan terjadi penurunan kualitas gambar. Nilai PSNR biasanya mempunyai rentang, nilai antara 20 dB sampai dengan 60 dB. Tabel 1 memperlihatkan nilai PSNR beserta penjelasannya.

TABEL 1 Nilai Peak Singnal to Noise Ratio

| **Rasio (dB)** | **Kualitas Citra** |
|---|---|
| 60 dB | *Excellent*, tanpa derau |
| 50 dB | *Good*, terdapat banyak derau tapi kualitas citra masih bagus |
| 40 dB | *Reasonable*, terdapat butiran halus seperti salju dan beberapa detail citra hilang |
| 30 dB | *Poor*, terdapat banyak derau pada citra |
| 20 dB | *Unusable* |

Berikut adalah sebuah tabel jangkauan yang digunakan untuk menentukan banyaknya bit yang akan disisipkan:

TABEL 2 Bit Yang Dapat Disisipkan Pada Daerah Rentang

| *R* (Rentang) | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| *bb* (batas bawah) | 0 | 8 | 16 | 32 | 64 | 128 |
| *ba* (batas atas) | 7 | 15 | 31 | 63 | 127 | 255 |
| *jb* (jumlah bit) | 3 | 3 | 4 | 5 | 6 | 7 |

Pada penelitian ini, PSNR digunakan untuk mengetahui perbandingan kualitas gambar sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai rata- rata kuadrat dari MSE (*Mean Square Error*). Perhitungan MSE adalah sebagai berikut:

$$MSE = \frac{1}{MN} \sum_{y-1}^{M} \sum_{x-1}^{N} [I(x,y) - J(x,y)]^2 \qquad (3)$$

Dari persamaan 3 memiliki keterangan yaitu, MSE adalah nilai dari citra stego. M sebagai panjang citra stego (dalam piksel). N sebagai lebar citra stego (dalam piksel). I(x,y) sebagai nilai piksel dari citra asli. J(x,y) sebagai nilai piksel dari citra stego. Sementara nilai PSNR dihitung dari kuadrat nilai maksimum sinyal dibagi dengan MSE.

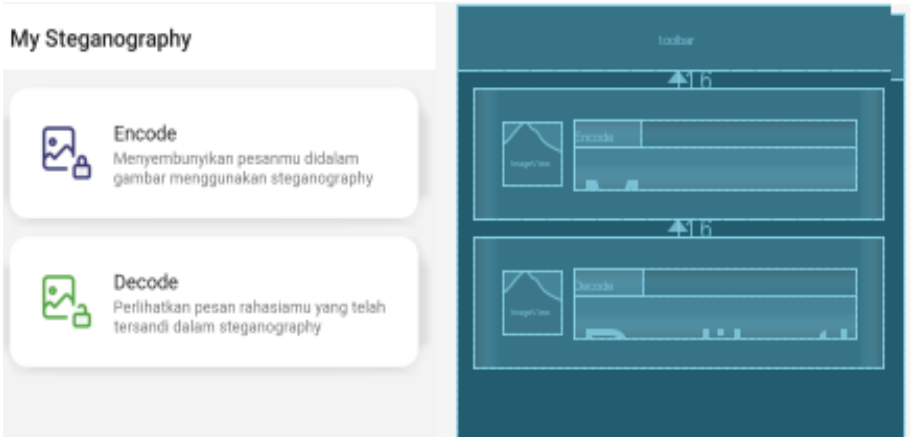
$$PSNR = 10 \; x \; log_{10} \left( \frac{MAXi}{MSE} \right) \qquad (4)$$

Pada persamaan 4 memiliki keterangan yaitu, PSNR adalah nilai dari citra. MAXi adalah nilai i maksimum piksel citra, dan MSE adalah nilai MSE.

## 4. Hasil dan Pembahasan

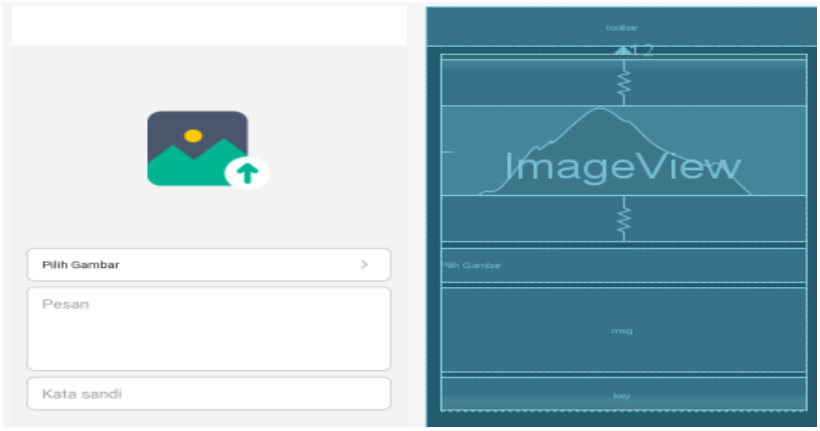
### 4.1 Perancangan Aplikasi

Rancangan aplikasi yang telah dibangun memiliki dua fungsi utama yang berada pada halaman utama yaitu fungsi encode dan fungsi decode. Halaman utama adalah halaman yang akan terbuka setelah splash screen selesai. Berikut adalah rancangan halaman utama pada gambar 5.



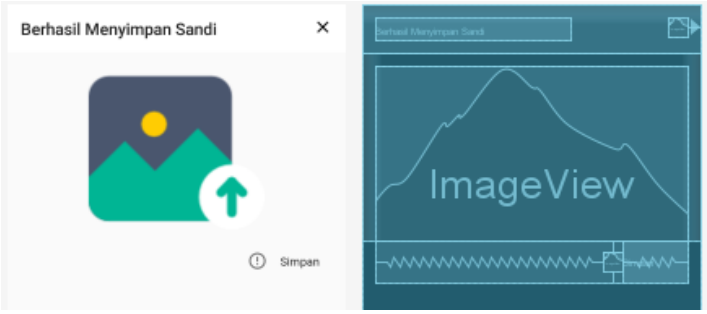

Gambar 5. Halaman Utama

Halaman utama pada gambar 5, memiliki dua menu yaitu encode dan decode. Menu encode adalah menu untuk mengalihkan ke halaman proses encode yang berfungsi untuk melakukan proses penyisipan pesan. Setelah pengguna memilih menu encode, maka akan berganti halaman encode seperti pada gambar 6.




Gambar 6. Halaman Encode

Pada gambar 6, halaman penyisipan pesan atau encode terdapat beberpa formulir yang wajib diisi pengguna untuk menggunakan fungsi encode tersebut. Tombol pilih gambar berfungsi untuk memilih gambar yang berada di penyimpanan, setelah memilih gambar yang diinginkan, maka icon gambar akan tergantikan dengan gambar yang telah terpilih. Formulir pesan berguna untuk menuliskan pesan rahasia yang ingin disisipkan pengguna. Formulir kata sandi berguna untuk menyimpan kata sandi yang akan digunakan untuk decode. Tombol encode berguna untuk melanjutkan ke proses encode setelah gambar dan formulir terisi semua. Ketika encode berhasil akan ditampilkan jendela baru seperti pada figure 7.



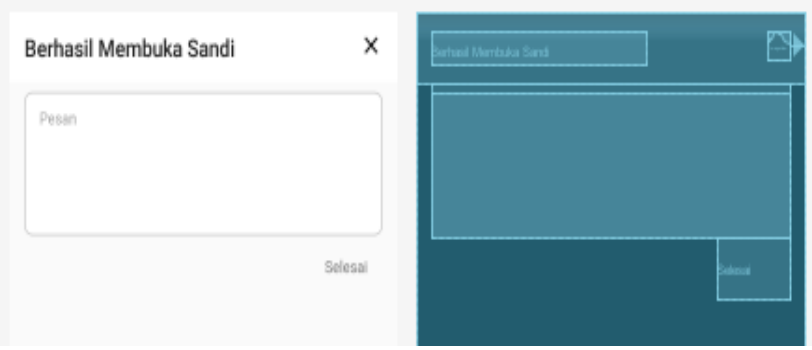

Gambar 7. Jendela Berhasil Proses Encode

Pada gambar 7 adalah tampilan jendela yang muncul setelah berhasil melakukan proses *encode*. Ikon gambar berfungdi untuk tempat ditampilkan *stego image*. Pada tombol ikon tanda seru berfungsi untuk menampilkan informasi lokasi penyimpanan *stego image* setelah di simpan. Tombol simpan berfungsi untuk menyimpan *stego image* ke *device* pengguna.

Menu kedua dari halaman utama adalah menu decode yang berfungsi untuk membuka *stego image*. Halaman decode dapat dilihat pada gambar 8.


Figure 8. Halaman Decode

Halaman decode pada figure 8 terdepat beberapa fitur untuk melakukan proses *decode*. Tombol pilih gambar berguna untuk memilih *stego image*. Pada formulir kata sandi berguna untuk memasukkan key atau kata sandi dari *stego image*. Jika *stego image* telah dipilih dan kata sandi telah terisi, tombol decode berguna untuk menjalankan proses *decode stego image*. Ketika proses *decode* berhasil sistem akan menampilkan jendela baru seperti pada figure 9.

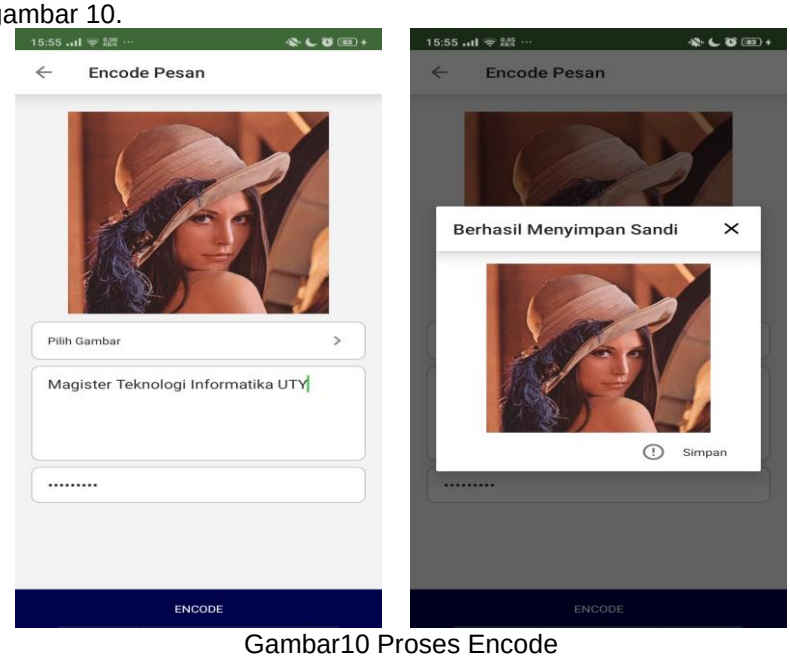



Gambar 9. Jendela Berhasil Proses Decode

Jendela berhasil decode pada gambar 9 akan menampilkan pesan yang tersisipkan dari *stego image* pada formulir pesan. Tombol 'X' dan tombol selesai berguna untuk mengeluarkan jendela. Tetapi, tombol selesai berguna juga untuk mengatur ulang gambar yang telah terpilih dan kata sandi yang dimasukkan sebelumnya akan dikosongkan.

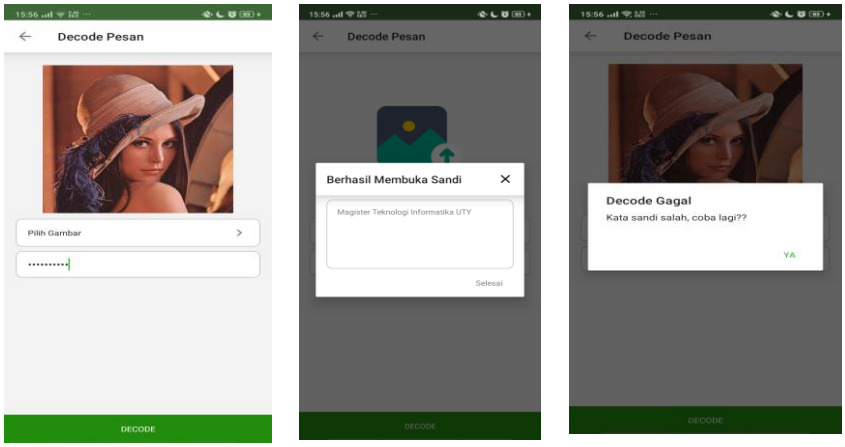
### 4.2 Pengujian Aplikasi

Berdasarkan algoritma yang diusulkan, peniliti mengembangkan sistem yang sederhana, dalam mengimplementasikan algoritma. Berdasarkan perancangan sistem seperti yang terlihat pada figure 2. Aplikasi mempunyai beberapa sistem yaitu mengelola proses *encode*, menghasilkan citra stego, mengelola proses *decode*, mengembalikan pesan rahasia pada citra stego (*decode*), dan keluar dari aplikasi. Adapun alur aplikasi pada proses encode terlihat pada gambar 10.




Gambar10 Proses Encode

Dari gambar 10, dilakukan proses *encode* setelah pengguna memilih citra dan mengisi pesan dan kata sandi. Jendela baru akan ditampilkan jika proses *encode* berhasil. Pengguna dapat menyimpan citra stego atau membiarkannya dengan memilih tombol 'X' pada jendela. Sedangkan, proses *decode* terlihat pada gambar 11.




Gambar11 Proses Decode

Proses decode pada gambar 11 dilakukan setelah pengguna memilih citra dan memasukkan kata sandi. Jendela baru akan ditampilkan jika proses *decode* berhasil. Jika proses decode gagal akan ditampilkan keterangan pada jendela decode gagal.

**4.3 Hasil Pengujian**

Pengujian sistem menggunakan citra seperti yang ditunjukkan pada figure. 12-13. figure. 12 (a) menunjukkan citra asli sebelum pesan disimpan di dalam citra dan Gambar. 12 (b) menunjukkan *stego image* setelah pesan disimpan di dalam citra. Peneliti menemukan bahwa *stego image* tidak memiliki distorsi yang nyata (seperti yang terlihat oleh mata telanjang).

Gambar 12 (a) Citra Asli

(b) Citra Stego

Dari Gambar 13 menunjukkan contoh citra lain dengan data yang disembunyikan di dalam citra. Dari figure. 13, menunjukkan bahwa perbandingan distorsi oleh mata telanjang antara citra sampul dan citra stego hampir nol. Permukaan di antara kedua gambar tidak menunjukkan perbedaan dengan menggunakan mata telanjang meskipun ukuran *stego image* sedikit lebih tinggi daripada citra aslinya.

Gambar13 (a) Citra Asli

(b) Citra Stego

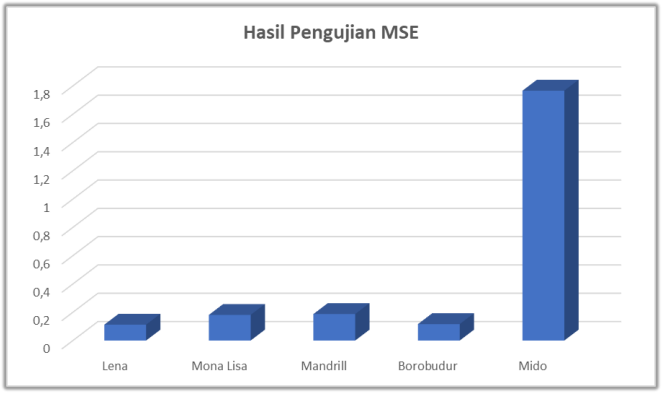
Pengujian MSE (*Mean Square Error*) dilakukan untuk menentukan nilai rata – rata kuadrat dari jumlah kuadrat *absolute error* antara *cover image* dengan citra stego, Sebelum

menentukan PNSR (Peak Signal to Noise Ratio). Hasil perhitungan MSE yang dilakukan dalam penelitian ini, dapat dilihat pada tabel 3.

TABEL 3 Pengujian MSE (*Mean Square Error*)

| No. | Nama Citra | Dimensi Citra | Ukuran Citra Stego | MSE |
|---|---|---|---|---|
| 1. | Lena | 512 x 512 | 96 kb | 0.112 |
| 2. | Mona Lisa | 450 x 681 | 90 kb | 0.181 |
| 3. | Mandril | 850 x 850 | 341 kb | 0.187 |
| 4. | Borobudur | 1200 x 849 | 372 kb | 0.116 |
| 5. | Mido | 378 x 496 | 94 kb | 1.766 |
| Rata – rata MSE | | | | 0.472 |

Dari pengujian yang telah dilakukan pada pengujian di atas, peneliti menggunakan grafik yang bertujuan menunjukan nilai MSE yang telah dilakukan. Berikut figure 14 grafik nilai MSE yang dihasilkan.




Gambar14 Proses Decode

Pengujian MSE yang telah dilakukan, menghasilkan nilai MSE dibawah 2 sehingga dapat dikatatakan baik. Sedangkan, pada pengujian algoritma dengan menggunakan PSNR (*Peak signal to noise ratio).* PSNR adalah pengukuran standar yang digunakan dalam teknik steganografi untuk menguji kualitas gambar stego. Semakin tinggi nilai PSNR, semakin tinggi kualitas gambar stego. Jika gambar sampul adalah C ukuran M × M dan gambar stego adalah S ukuran N × N, maka setiap gambar sampul C dan gambar stego S akan memiliki nilai piksel (x, y) dari 0 hingga M-1 dan 0 untuk N-1 masing-masing. Hasil perhitungan PSNR yang dilakukan dalam penelitian ini, dapat dilihat pada tabel 4.

TABEL 4 Pengujian PSNR (*Peak Signal to Noise Ratio*)

| No. | Nama Citra | Dimensi Citra | Ukuran Citra Stego | PSNR |
|---|---|---|---|---|
| 1. | Lena | 512 x 512 | 96 kb | 57.651 dB |
| 2. | Mona Lisa | 450 x 681 | 90 kb | 55.562 dB |
| 3. | Mandril | 850 x 850 | 341 kb | 55.405 dB |
| 4. | Borobudur | 1200 x 849 | 372 kb | 57.501 dB |
| 3. | Mido | 378 x 496 | 94 kb | 45.662 dB |
| Rata – rata PSNR | | | | 54.356 dB |

Berdasarkan pengujian MSE dan PNSR didapatkan bahwa nilai rata-rata MSE yang dihasilkan kurang dari 1 dan rata-rata PNSR diatas 50 dB, berarti perubahan kualitas warna antara citra asli dengan citra stego tidak mengalami perubahan yang signifikan, sehingga keberadaan dari file yang tersembunyi tidak mudah di deteksi oleh indra penglihatan manusia.

## 5. Kesimpulan

Hasil pengujian yang dilakukan, didapatkan bahwa proses pengamanan data menggunakan steganografi dengan metode DCT berhasil diintegrasikan dan diterapkan dengan hasil yang baik pada aplikasi mobile berbasis android. Aplikasi mobile yang menerapkan dua

fungsi utama steganografi yaitu teknik encode dan teknik decode. Pada pengujian menggunakan 5 sampel citra asli dan 5 sampel citra stego yang tiap dimensi berbeda. Pada proses encode citra asli sebagai *cover* berhasil disisipkan pesan rahasia. Sedangkan, proses decode dapat mengembalikan ukuran pesan dan isi pesan dengan baik. Dilakukan juga pengujian terhadap citra stego dengan menggunakan MSE dan PSNR. Berdasarkan pengujian menggunakan algoritma *mean square error* (MSE) menghasilkan nilai rata-rata sebesar 0.472 dan pengujian menggunakan algoritma peak *signal to noise ratio* (PSNR) menghasilkan nilai rata-rata sebesar 54.356 dB.

Saran yang dapat diberikan untuk pengembangan lebih lanjut dari aplikasi steganografi yaitu, diharapkan pada penelitian selanjutnya untuk dapat menggunakan kriptografi pada pesan rahasia sebelum disisipkan kedalam citra stego dan diharapkan aplikasi steganografi dapat menggunakan semua file selain format citra untuk dijadikan *cover stego*.

**DAFTAR REFERENSI**

[1] PourArian, M.R., Hanani, A. Blind Steganography in Color Images by Double Wavelet Transform and Improved Arnold Transform. *Indones J Electr Eng Comput Sci*. 2016; 3(3): 586–600.
[2] Malathi, P., Gireeshkumar, T. Relating the Embedding Efficiency of LSB Steganography Techniques in Spatial and Transform Domains. In: *Procedia Computer Science*. 2016.
[3] Bhasme, S., Abu, A., Gandhi, K., & Phadnis, R. Visual Cryptography and Steganography Techniques for Secure E-Payment System. *Int Res J Eng Technol*. 2016; 3(3): 1018–21.
[4] Yunus, M., Harjoko, A. Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT. *Indones J Comput Cybern Syst*. 2014; 8(1): 81–90.
[5] Kalita, M., Tuithung, T. A Comparative Study of Steganography Algorithms of Spatial and Transform Domain. *IJCA Proc Natl Conf Recent Trends Inf Technol*. 2015; (Ncit): 9–14.
[6] Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E., & Mohamed, E. A secure image steganography algorithm based on least significant bit and integer wavelet transform. *J Syst Eng Electron*. 2018; 29(3): 639–49.
[7] Setiadi, D.R.I.M., Rachmawanto, E.H., & Sari, C.A. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *J Appl Intell Syst*. 2017; 2(1): 1–11.
[8] Shalini, V., Sreeja, E., & Veluchamy, M. Implementation of Multi-Party Key Authentication and Steganography for Secured Data Transaction in Cloud. *IJSRST*. 2016; 2(2): 56–60.
[9] Sidik, F., Wamiliana, Febriansyah, E. Perbandingan Metode Adaptive Minimum Error Least Significant Bit Replacement (Amelsbr) Dan Discrete Cosine Transform (Dct) Untuk Steganografi Citra Digital. *J Komputasi*. 2018; 6(1): 43–53.
[10] Garno, G., Solehudin, A. Teknik Steganografi dengan Metode Discrete Cosines Transform (DCT) pada Citra Interpolasi Bilinear untuk Pengamanan Pesan. *J Inform Upgris*. 2017; 3(2): 116–21.
[11] Saidah, S., Ibrahim, N., & Widianto, M.H. Pengamanan Pesan pada Steganografi Citra dengan Teknik Penyisipan Spread Spectrum. *ELKOMIKA J Tek Energi Elektr Tek Telekomun Tek Elektron*. 2019; 7(3): 544-558.
[12] Zulfikar, D.H., Harjoko, A. Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapan Point Operation Image Enhancement. *IJCCS (Indonesian J Comput Cybern Syst*. 2016; 10(1): 35-46
[13] Setiadi, D.R.I.M., Handoyo, A.E., Rachmawanto, E.H., Sari, C.A., & Susanto, A. Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *J Teknol dan Sist Komput.* 2018; 6(1): 37-43.
[14] Sinduningrum, E., Supriyanto, A. Perancangan Aplikasi Steganografi Berbasis Android dengan Metode Pixel Value Differencing (PVD). *Multinetics*. 2016; 2(2): 16-23.
[15] Yunus, M., & Harjoko, A. Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*. 2014; *8*(1): 81-90.
[16] Garno, G., Solehudin, A. Teknik Steganografi dengan Metode Discrete Cosines Transform (DCT) pada Citra Interpolasi Bilinear untuk Pengamanan Pesan. *J Inform Upgris*. 2017; 3(2): 116–121.